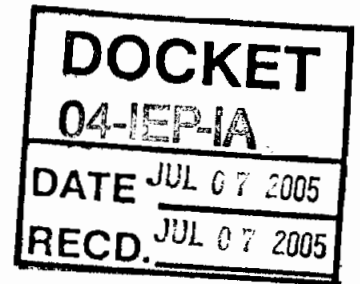




**Western States Petroleum Association**  
Credible Solutions • Responsive Service • Since 1907



**Joe Sparano**  
President

July 7, 2005

Mr. John Geesman  
2005 Integrated Energy Policy Report (Energy Report) Committee  
California Energy Commission  
1516 Ninth Street  
Sacramento, CA 95814-5512

Mr. Jim Boyd  
2005 Integrated Energy Policy Report (Energy Report) Committee  
California Energy Commission  
1516 Ninth Street  
Sacramento, CA 95814-5512

**Subject: Western States Petroleum Association Comments on the CEC, 2005  
Petroleum Infrastructure Environmental Performance Report (EPR):  
Docket 04-IEP-1A**

On behalf of the Western States Petroleum Association (WSPA), we appreciate the opportunity to express our industry's view, comments and suggested recommendations on the draft California Energy Commission's (CEC) 2005 Infrastructure Environmental Performance Report (EPR). WSPA is a non-profit trade association that represents petroleum companies that explore for, produce, transport, market and refine petroleum and petroleum products in California and five other western states.

WSPA is pleased that the draft EPR has generally given our industry a good environmental performance rating for the years reviewed [1985 – 2004], and that it acknowledges the continuing trends in pollution reduction and environmental improvements that are occurring across all environmental media for our industry.

We agree with CEC statements in the EPR that petroleum and petroleum products are integral and critical parts of the California economy. We believe that CEC has a vital role to ensure that the petroleum infrastructure needed to meet California's ever-growing demand will continue to be available, in view of the increasingly stringent environmental restrictions and demands placed on facilities.

WSPA has conducted a review of the EPR, and in addition to our oral testimony submitted during the June 20, 2005, EPR Committee Workshop, we are submitting the following written comments.

Our comments are divided into two main sections. The first section includes Key Policy Comments that we believe are critically important for the CEC to understand and act on from an overall Policy standpoint. The second section focuses on Specific comments, concerns and recommendations within each Chapter of the EPR and is contained as a separate Attachment 1.

## **KEY POLICY COMMENTS**

### **1. CEC's Main Priority:**

First and foremost, we believe the CEC should place its highest priority on helping to ensure California consumers have reliable and affordable access to energy supplies. Additionally, the CEC has no specific statutory requirement or mandate for developing the EPR for our industry. In fact, most of the issues addressed in the EPR are the responsibility of Cal-EPA and its agencies to address these issues from an environmental and health impact perspective.

However, despite these facts, WSPA does recognize and understands the importance for the CEC to engage in the dialogue and review of the environmental, public health and safety issues that could severely impact the viability of existing facilities and development and expansion of new petroleum infrastructure.

### **2. Need for Affirmative Policy Actions and Recommendations:**

The CEC has identified critical petroleum infrastructure needs in the IEPR and has provided a look to the future to determine if environmental issues could affect projected expansion of petroleum infrastructure needed in the EPR. Based on information from these two reviews, the EPR should: contain more *Affirmative Policy Actions and Recommendations* that will minimize obstacles; and, provide balance between energy infrastructure needs and environmental priorities to ensure existing infrastructure is maintained and opportunities for infrastructure enhancements are actually accomplished. We have provided specific Recommendations and areas that we urge the CEC provide specific Policy Actions in our comments.

WSPA recognizes that the CEC has been supportive in the past of removing or reducing barriers in an effort to protect existing infrastructure and to provide additional energy infrastructure. We believe the EPR should give the CEC a high degree of comfort that the trends in environmental performance provide the necessary evidence and protection to allow the CEC to develop affirmative policies, actions and recommendations that support its efforts to protect and expand the state's petroleum infrastructure.

**3. Need for Clear Differentiation of Marine Petroleum Infrastructure Facilities and Review of Emission Calculations**

In several sections of the EPR, there are references and statements that attribute environmental issues and concerns of marine ports with petroleum infrastructure facilities. Staff needs to review carefully and differentiate between who produces the fuel versus who uses the fuel and how the two are correctly linked to the term "petroleum infrastructure."

Additionally, WSPA recommends staff should clearly differentiate and calculate the emissions associated with petroleum infrastructure facilities versus emissions from other sources that are not petroleum infrastructure related, such as cargo container equipment, rail locomotives, trucks and cranes. Finally, as we stated during the workshop, we are concerned and question whether emissions from "petroleum related shipping activities" that are 200 miles off the coast, are appropriately associated with petroleum infrastructure facilities. These issues need to be further reviewed to determine whether they are appropriate and applicable to the petroleum industry.

**4. Support for Partnerships:**

WSPA agrees with the Staff report on the desirability of partnerships, and supports the Commission's goal of educating stakeholders on the need for petroleum infrastructure upgrades to meet future demand for transportation fuels. We support the staff's recommendation of reducing energy usage wherever it is economically and technically feasible, and with the priority of increasing energy efficiency.

**5. Need for review of Data/Information:**

As mentioned above, WSPA recognizes the importance of the CEC engaging in the dialogue and review of the environmental, public health and safety issues that could impact the viability of existing facilities, and development and expansion of new petroleum infrastructure. However, we have identified several issues and concerns and included specific recommendations staff should undertake to make the EPR more accurate. Our specific comments are listed in Attachment 1. Additionally, given our issues and concerns with the EPR, we recommend staff should have the Cal-EPA agencies review the EPR as well, in order to improve its accuracy.

6. **Environmental Justice (EJ):**

While WSPA supports the CEC becoming involved in joint EJ projects with other agencies, we would only caution that CEC should not unnecessarily duplicate EJ program efforts by Cal-EPA. Instead, CEC should ensure Cal-EPA and its agencies understand the current and future energy demands, supplies and petroleum infrastructure needs so that they can be carefully balanced with EJ and environmental issues.

In closing, although WSPA appreciates the CEC extending the time deadline to July 7, 2005, please note that we may provide additional or clarifying comments beyond the July 7, 2005 deadline date, since this is a complicated and critically important issue for California.

If you have any questions, or need additional information, please contact Ms. Gina Grey at (480) 595-7121 or me at (916) 498-7754.

Sincerely,

A handwritten signature in black ink that reads "Joe Sparano". The signature is written in a cursive, flowing style.

cc: Mr. Joe Desmond – Chairman, CEC  
Mr. Chris Tooker - CEC

# ATTACHMENT 1

## Specific Chapter Comments

### 1. CHAPTER 1 - INTRODUCTION:

#### Chapter 1 – Findings Section, WSPA Support:

- WSPA strongly supports the EPR's recognition that California's petroleum industry and the "diverse products that it produces" are critical to the state's economy. In addition, as the demand for these products continues to increase, the state's petroleum infrastructure will need to be "modernized and expanded".
- WSPA supports the EPR finding the need for increased imports of crude and petroleum products, will come mostly from foreign sources, and will therefore result in the need for new marine terminals and storage infrastructure facilities.
- WSPA concurs with the finding that petroleum infrastructure construction and expansion activities are difficult to plan. Additionally, it is difficult to permit and build projects due to available land in existing port and refinery locations as well as land-use conflicts and challenges by surrounding communities.
- WSPA concurs with the fact that communities surrounding refineries are concerned about a variety of environmental, health and safety impacts related to the operation of oil refineries and infrastructure related operations. As correctly noted in the EPR, Federal, State and local agencies are actively implementing Environmental Justice policies, programs and activities to address community concerns and issues. Please refer to page 15 below for more specific comments regarding Environmental Justice.
- WSPA agrees with the finding that some refineries have experienced accidental releases and supports staff's statements that:  
  
*"Petroleum infrastructure facilities have, for the most part, effectively managed their use of hazardous materials such that they do not pose a significant safety or health risk to local communities".*
- WSPA concurs with the finding that the petroleum industry does take seriously its responsibility to remediate petroleum spills and releases, and that the potential for future releases will be reduced.

WSPA supports the finding and recognition that tanker oil spills into water bodies has declined since 1986, as has the volume of oil spilled.

In addition to a minimal environmental impact, WSPA would also like to point out in regards to offshore oil production and product movement in the Central Coast region there is strong evidence that a vibrant tourism economy has grown alongside oil and gas industry activity

Total visitor volumes, travel spending, travel industry earnings, employment and tax revenues all continue to increase in both Ventura and Santa Barbara Counties.

## **Chapter 1 – Findings Section - WSPA Concerns / Recommendations:**

- ***Air Pollutant Emissions:*** The EPR noted that air pollutant emissions from the petroleum industry have declined since 1975 due to new air quality regulations and rules, however, the report should also recognize the many modernization and efficiency investments and procedural upgrades that refinery operators have implemented since the facilities were built – not always as a result of government regulation – but nonetheless resulting in environmental improvements for Californians.
- ***Refinery Flaring:*** While WSPA understands that refinery flaring is a concern to communities near refineries, we believe it is important that the finding reflect the fact that Air Districts have recognized there is no such thing as “routine flaring”. Flares exist as emergency safety devices for refineries and do not operate on a routine basis. Please refer to page 19, for specific comments on refinery flaring and recommendations.

**Recommendation:** WSPA recommends staff include in this section the following statement:

*“Refinery flaring exists as an emergency safety device and does not operate on a routine basis” Refinery flares are designed in accordance with federal standards to safely burn gases that cannot be recycled for use as fuel. In addition, in the South Coast, refineries have reduced by more than 80% flare emissions for sulfur oxides since the SCAQMD first required monitoring of flare emissions. In the Bay Area, smog forming emissions from flaring, measured with equipment and methodology required by the BAAQMD, represent less than 1/1000<sup>th</sup> of the region’s smog forming emissions”.*

- ***Marine Terminal and Refinery Emissions:*** WSPA disagrees with staff’s finding that for future marine terminal and refinery emissions, only the Bay Area air district is “...projecting increases in air emissions from petroleum infrastructure”. In discussing this matter with Mr. Jack Broadbent of the Bay Air Quality Management District (BAAQMD), he was surprised with this finding as well and was interested in discussing this matter further with the CEC.

**Recommendation:** WSPA urges the CEC to discuss the above finding with the BAAQMD to clarify and report correctly the state of air emissions from petroleum infrastructure facilities. WSPA would be pleased to assist in coordinating a meeting with the CEC and BAAQMD.

- ***Marine Terminals Petroleum Infrastructure:*** WSPA is concerned that staff are characterizing Marine terminals as petroleum infrastructure facilities, when petroleum-related marine activities are only a piece of the equation. In the discussions of marine emissions, it would appear emissions from anything that operates in the marine environment that burns petroleum gets “lumped” into “petroleum infrastructure.”

In reality, these emissions are a consequence of other operations and activities that take place in the marine environment. The report unfortunately appears to mix diesel’s use as a fuel in the transportation sector, with its utilization throughout the petroleum infrastructure. We believe staff should clearly identify those sources that cannot be defined as associated with petroleum infrastructure activities, such as diesel trucks, cranes, cargo container equipment and rail locomotives. However, activities and equipment such as ocean going vessels (oil tankers), tug and barges, pipeline and associated pumps and storage tank facilities are clearly petroleum infrastructure related activities.

**Recommendation:** WSPA recommends staff revise the section on Marine Terminals and clearly differentiate the emissions associated with petroleum infrastructure facilities verses emissions from other sources that are not petroleum infrastructure related, such as cargo container equipment, rail locomotives, trucks and cranes, simply because they use petroleum based fuels.

- ***Safety and Security:*** WSPA members take very seriously the issue of safety and protection against terrorist threats. In fact, WSPA members in association with the American Petroleum Institute (API) have been on the forefront of developing security guidelines for the petroleum industry. API has just recently released (April, 2005) a guidance document entitled Security Guidelines for the Petroleum Industry as well as other supporting papers and guidelines that provides necessary security and safety guidance against terrorism for the petroleum industry as well as applicable regulatory agencies. WSPA continues to work closely with the US Coast Guard (U.S.C.G.), the Department of Interior, Minerals Management Services (MMS) and various law enforcement agencies to maintain and enhance facility and personnel safety and security. Of particular note, WSPA and the U.S.C.G. are finalizing work on amending regulations pertaining to Pacific Offshore Platform Safety Zones to require small vessel notification/identification procedures when approaching these facilities.

In addition, WSPA and the MMS have jointly produced a “Platform Protection Guidance Document” for use by the Pacific Offshore Petroleum Industry.

**Recommendation:** WSPA recommends staff re-evaluate the section regarding the state of emergency preparedness and response as it applies to the petroleum industry. As

stated previously, there are extensive Safety and Security measures for petroleum infrastructure facilities in place both at the Federal and State level. Appendix 1, contains reference materials and information on this subject matter for further reference and review by staff. WSPA urges staff incorporate and reference this information in the final EPR report, so the reader understands the current state of Federal and State security programs that are in place today.

- **Hazardous Waste Generation:** WSPA disagrees with staff's finding that data on hazardous waste generation and management is "inconsistent and often lacking for petroleum infrastructure facilities".

WSPA members take seriously the responsibility for handling, transporting and disposing of all hazardous waste materials.

**Recommendation:** WSPA requests staff revise this finding and recommends the following revision:

*"The petroleum industry manages hazardous waste materials in accordance with Federal, State and local agency laws and regulations. Any material deemed as hazardous is subject to strict State hazardous waste manifest documentation and reporting requirements mandated by the State Department of Toxic Substances Control (DTSC). Further, the petroleum industry has been a leader in the field of hazardous waste pollution prevention and reduction. For example, implementation of the SB 14 source reduction program, which has a baseline year of 1986, has resulted in the petroleum industry reducing the amount of generated hazardous waste by over 75%."*

Please refer to page 22 for more specific comments regarding the Hazardous Waste and Generation Section of the EPR.

- **Dredging Activities:** WSPA has concerns with staff's finding that Dredging to allow tanker traffic and terminal development can increase sedimentation in the bays and waterways and subsequently impact biological communities.

The Report failed to reference the fact that dredging activities are extensively regulated and permitted by a comprehensive list of federal, state and regional agencies in California. Specifically, these agencies include: the U.S. EPA, U.S. Army Corps of Engineers, San Francisco Bay Regional Water Quality Control Board, and the San Francisco Bay Conservation and Development Commission.

In 1990, these agencies came together to form a collaborative program called the: Long Term Management Strategy (LTMS) program, with the mission of specifically focusing on dredging activities and management of dredging materials in the San Francisco Bay Area. Extensive permitting requirements and reviews focus on the impacts dredging will have on the biological community of the Bay, as well as the beneficial uses of dredged materials.



As we stated in our oral comments during the June 20<sup>th</sup>, 2005 EPR workshop, dredging ship channels and refinery terminals is critical for providing safe access for incoming crude tankers and cargo ships to meet the increasing demand for petroleum fuels in California.

**Recommendation:** WSPA recommends staff revise this Finding and incorporate reference to the multitude of regulatory agencies and their regulatory oversight and the permitting processes required, before operators are allowed to dredge San Francisco Bay. Further, we urge the CEC to also emphasize the importance of providing secure, safe and consistent access to shipping channels so that oil tankers can deliver crude oil to refineries.

Please refer to page 31 comments and recommendations on the issue of dredging.

- **Ballast Water:** In general, WSPA supports staff's Ballast Water finding which stated the following:

*"Discharge of ballast water from tankers (an all ocean-bound ships) has caused the introduction of non-indigenous species into California waterways. Aggressive regulations and programs underway by the State Lands Commission should limit further introductions"*

We have several concerns with several statements in Chapter 10. Please refer to page 29 for our specific concerns.

#### **Chapter 1 – Policy Options Section, WSPA Support:**

- ***Need for Timely Information to allow Expansion or Modification of Petroleum Infrastructure Facilities:*** WSPA strongly supports staff's policy recommendation for the need to provide timely information to facilitate the plans and processes necessary to allow the expansion and construction of petroleum infrastructure operations. We also support the recommendation to identify opportunities for increased energy efficiencies as well as the alternative use of materials such as petroleum coke.
- ***Support of CARB's Efforts to Develop Siting Criteria:*** WSPA supports CEC's recommendations to support the Air Resource Board's efforts to develop petroleum infrastructure siting criteria for use by local land use agencies. In fact, as noted in Chapter 3, Land Use, staff references the recently adopted a land use guidance manual entitled: "Cal-EPA, *Air Quality and Land Use Handbook: A Community Health Perspective*", dated March, 2005 . This Handbook is an excellent Guidance document that describes general criteria that can be use by land use planners and regulatory agencies when siting land use developments and avoid land use conflicts, particularly near industrial and petroleum infrastructure facilities.
- ***Support CEC efforts to work with Local Air Districts:*** WSPA supports CEC efforts and recommendations to work with the ARB and local air districts to address differing

methodologies to quantifying air pollutant emissions from ports, refineries and other sources. We also note that the air districts and the ARB already possess the necessary expertise, skill and knowledge to quantify emissions and emission inventories within their regulatory regions. With a better understanding of the emissions inventory and cost-effective control strategies, efforts done in partnership with all stakeholders should facilitate the expansion of petroleum infrastructure facilities.

## **Chapter 1 - Policy Options Section, WSPA Concerns / Recommendations:**

- ***Efforts by ARB to Reduce Diesel Particulate Matter:*** WSPA supports the CEC engaging in a dialogue on particulate matter (PM) emissions from shipping activities associated with marine terminals. However, we would like to point out that the California Air Resources Board (CARB) as well as other agencies are not only focusing on diesel PM emissions from marine terminals, they have been actively implementing a diesel and PM emission reduction plan since 2000, called the “*Risk Reduction Plan to Reduce Particulate matter Emissions from Diesel-fueled Engines and Vehicles (Plan)*”.

The Plan’s goals are to reduce diesel PM by 75% by 2010 and an 85% reduction by 2020 from the 2000 baseline. Besides the ARB, the South Coast AQMD is also working with Ports and marine facilities to better characterize the amount of diesel PM and other criteria air pollutants and is implementing a comprehensive program to address diesel exhaust and PM emissions.

**Recommendation:** WSPA recommends the CEC include references to CARB’s current efforts to address diesel particulate matter emissions.

- ***Partnering with the Department of Toxics Substances Control:*** Although WSPA supports CEC’s Policy Option to partner with industry and other agency and stakeholder groups to examine process improvements to reduce hazardous waste within the petroleum industry, we believe such collaboration and partnering has and is currently taking place with the Department of Toxics Substances Control (DTSC). As described in more detail on page 27, WSPA members comply with the strict documentation and reporting requirements when dealing with the storage, handling and disposal of hazardous waste materials.

**Recommendation:** WSPA recommends CEC revise the hazardous waste Policy Option to reflect industry’s efforts in reducing and implementing pollution prevention programs such as SB14, that since its baseline year 1986 have resulting in a 75% reduction of hazardous waste materials.

## 2. CHAPTER 2 – CALIFORNIA’S PETROLEUM INDUSTRY INFRASTRUCTURE

### Chapter 2 - WSPA SUPPORT:

***Petroleum Infrastructure Will Require Expansion of Marine Terminal Capacity:*** WSPA supports CEC’s efforts in describing the overall landscape of the petroleum infrastructure problems and challenges we face in this state to keep up with the growing demand for transportation fuels. We support CEC’s statement that California's infrastructure will require expansion of marine terminal capacity, storage and the gathering pipelines that connect marine facilities and refineries to main product pipelines.

We also appreciate the fact that the CEC recognizes that California is a “fuel island” and although California’s gasoline is considered the cleanest burning in the world, it comes at a cost.

Additionally, we appreciate the fact that staff has noted, as we have in many EPR forums prior to this one, that refinery closures in California since 1985 have reduced operating refineries from 35 to 13.

***Staff Findings and Policy Options:*** On page 24, staff lists out specific Staff Findings and Policy Options. WSPA supports staff’s findings and policy options and specifically have the following comments:

- WSPA agrees that demand will continue to rise, even with “initiatives to reduce dependency on petroleum”.
- WSPA agrees that new fuel specifications will require more modification, which in turn will require additional equipment upgrades, process modifications and ultimately timely resolution and certainty in the permitting process.
- Although we can't predict whether there will be increases in refining capacity, we would add that it is certainly our members hope that if the investment climate in California improves, it would encourage investments and opportunities to expand refining capacity
- WSPA agrees there will most likely be increased imports of petroleum and petroleum products.
- WSPA agrees that the CEC may want to discuss with the State Fire Marshall the state of existing pipelines and if they need to be reviewed to determine if the pipeline infrastructure is indeed aging and poses a concern

**Recommendation:** As mentioned above, WSPA appreciates staff’s analysis and more importantly supports the Findings and Policy Options listed on page 24 of the EPR. WSPA does recommend however, that the CEC should go beyond the Findings and Policy Options and provide specific *Policy Actions* necessary to ensure California is able to meet not only their current, but future energy supply demands in the coming years.

Clearly, staff has done an excellent job of identifying the specific issues and needs. Again, we urge the CEC to go further and identify the specific actions necessary that can be put into action to ensure sufficient energy supplies in the future.

## **Chapter 2 - California's Petroleum Industry Infrastructure:**

### **WSPA Concerns / Recommendations**

***National verse California Refinery Closure Rates:*** On page 16, the EPR states refinery closure rates are close to the national average, implying that California is not very different from the rest of the nation. Although the percentage of refinery closures may be similar, there is a significant difference between the rest of the nation and California in terms of capacity --- the national capacity has increased, while total California refining capacity has decreased.

Even so, it should be recognized that the 13 remaining refineries in CA have maximized refining efficiency and utilization rates despite the enormous challenges presented by market driven increased demand for petroleum products.

This increased utilization, has occurred despite a historically poor rate of return on domestic refining and downstream investments (based on publicly available information including the U.S. Energy Information Administration, Standard & Poors, U.S. Bureau of Labor Statistics and American Petroleum Institute).

**Recommendation:** WSPA recommends the CEC revise this section and include reference to the fact that although the national refinery capacity has increased and total California refining capacity has decreased, the report should reflect that California's 13 remaining refineries have maximized refining efficiency and utilization rates, in the face of enormous increased demand for petroleum products.

***Projected Petroleum Storage Capacity Need by 2015 and 2025:*** On page 23 of the Report, the CEC projected over the next 20 years, demand for petroleum storage capacity for the San Francisco Bay Area and the Los Angeles/Long Beach regions will be necessary to meet the rising fuel energy demands of California. Specifically, it was noted that by 2015, the San Francisco Bay Area and Los Angeles/Long Beach could require between 0.8 and 1.6 million barrels and 1.2 to 2.4 million barrels of additional storage capacity and by 2025, the additional increased capacity is estimated to range from 1.2 to 2.4 and 4.8 to 9.3 million barrels.

**Recommendation:** WSPA appreciates the CEC recognizes the petroleum storage capacity needs California will face in the next 20 years in order to meet the rising fuel energy demands. Unfortunately, no-where in the EPR or related documents does it specifically list the necessary policy and regulatory actions that must be undertaken to avoid the projected storage capacity shortfall issues that California will face in the next 20 years.

WSPA recommends the CEC should identify the specific recommendations and actions that will be necessary to adequately address the petroleum storage capacity needs for California in the next 20 years.

***Pinole Shoal Dredging:*** On page 23, WSPA appreciates the fact that staff identified an issue of great concern to our members, which is the challenge of securing federal funding in a timely and reliable manner to ensure the dredging of the Pinole Shoal can occur. This is important, so that the movement of marine vessels through the Carquinez Strait can occur on a reliable schedule. Clearly, the ability to ensure continued movement of crude oil tankers to refineries is critical towards meeting the energy and fuel supply demand for California.

**Recommendation:** WSPA recommends the CEC should identify specific recommendations and actions necessary to ensure Pinole Shoal dredging activities can occur in a timely and reliable manner. We suggest specific actions may include, providing the legislative/regulatory support necessary to securing federal funding for dredging activities on a timely and certain basis, provide the necessary documentation and information needed regarding the current and future energy growth needs of California.

This would highlight the critical importance of ensuring the transportation and delivery of petroleum crude oil and blend stocks is done on a timely and reliable schedule to refinery locations, not only in the Bay Area, but also throughout California and the West Coast.

***California's New Source Review (NSR) Requirements:*** WSPA would like to raise an issue that we believe is important for the EPR to address. California has its own unique New Source Review (NSR) permitting standards and requirements. Most other states operate under the National NSR program that does not require BACT for all NSR permits. In short, California's NSR program requires additional, more stringent permitting requirements and standards above and beyond the National standards, which poses additional challenges and difficulties in obtaining necessary permits for refinery modification and expansion projects. However, under the National NSR standards and regulations, refineries would be able to implement expansion projects on a more timely and certain basis, without compromising the environment or air quality standards.

**Recommendation:** Although WSPA understands that California has the strictest environmental standards in the nation; it is equally important that the CEC must play a key role towards balancing environmental protection and ensures that California can meet the ever-increasing energy demands. In that regard, WSPA recommends the CEC incorporate the following language into the EPR:

*"California NSR requirements might actually prevent reduction of emissions because some upgrades that are less than Best Available Control Technology (BACT) could reduce current emissions, comply with federal NSR requirements, and increase petroleum infrastructure, but are precluded by the unique California standards. The result could be higher emissions, less petroleum products, and other negative environmental consequences". The CEC should consider initiating discussions on this issue".*

### 3. CHAPTER 3 – LAND USE

#### Chapter 3 - WSPA Support:

WSPA commends staff for putting into proper context the history and development of the petroleum infrastructure in California. As noted in the Introduction, petroleum refineries and infrastructure was developed decades ago in areas that were relatively remote from urban areas. Consequently, as the state's population expanded, communities developed near petroleum infrastructure facilities, resulting in land use issues and conflicts.

WSPA has a long history of supporting a more coordinated approach to land-use planning and decision making for future development near existing petroleum infrastructure facilities. As noted in your report, WSPA participated with the California Air Resources Board (CARB) in the development and support of the "*Air Quality and Land Use Handbook: A Community Health Perspective*".

#### Chapter 3 – Land Use: WSPA Concerns / Recommendations:

***Marine Terminals/Storage Terminals:*** As we stated previously on page 5, WSPA is concerned that staff are characterizing Marine terminals as petroleum infrastructure facilities, when petroleum-related marine activities are only part of marine terminals.

We would like to reiterate our recommendation that staff should clearly identify those sources that cannot be defined as associated with petroleum infrastructure activities, such as diesel trucks, cranes, cargo container equipment and rail locomotives, with equipment that is considered petroleum infrastructure such as ocean going vessels (oil tankers), tug and barges, pipeline and associated pumps and storage tank facilities.

***Growth Projections:*** On Page 27, staff references a recent study that based on "current" growth projections estimated the ports of Los Angeles and Long Beach will require over 5,000 new acres for container operations by 2010 and an additional 9,400 new acres by 2020. This estimate is for container operations alone and without any consideration of the potential space needs for new and expansion for new, existing, or expansion of existing petroleum infrastructure facilities.

The issue of building new and expanding existing marine petroleum infrastructure facilities is a very important one to our members, especially given the challenges and issues we face in many local and regional areas regarding maintaining, let alone, expanding, critical petroleum infrastructure facilities.

***Port of Los Angeles Community Advisory Committee (PCAC):*** As an example, on June 21, 2005, the Port of Los Angeles Community Advisory Committee (PCAC) passed a motion urging the Board of Harbor Commissioners direct Port staff to develop a plan, that includes an implementation schedule and site identifications, for the *relocation* of all liquid bulk handling and storage facilities at the Port.

This motion and subsequent report could have a severe impact on the ability of WSPA member companies to adequately handle the supplies that will be needed to meet the increasing demand for petroleum fuels

In addition, on June 22, 2005, the Board of Harbor Commissioners voted unanimously (4-0) to end the lease for the Amerigas bulk storage facility at Berth 120 in the Port of Los Angeles, and to terminate its pipeline franchise, which services two critical adjunct, refining facilities in the region. Clearly this local regulatory decision will negatively impact both existing product storage and goods movement in the region.

The action by the Board of Harbor Commissioners provides a real time example of the challenges and decisions local entities are posing on the current and future investments of petroleum infrastructure facilities in Southern California.

WSPA supports staff's recognition that given the projected growth and demand for petroleum fuels, there will be a need for increased importation of crude oil and petroleum products. Subsequently, this will require an increased need in building and expanding on existing marine petroleum infrastructure facilities.

**Recommendation:** Given the need for increased demand for the importation of petroleum and its products, and additional land to build new and expand existing marine petroleum infrastructure and storage facilities, it is critically important the CEC take action and establish a policy to ensure critical petroleum infrastructure facilities are maintained and given a high priority so that the current and future energy needs of this State are met. This is even more evident today, given the recent actions of local entities such as the Board of Harbor Commissioners on the Amerigas leasing issue.

The Policy Actions should reference the importance and need for new and expansion of existing petroleum infrastructure facilities to ensure California meets its increasing fuel needs.

### **3. CHAPTER 4 – ENVIRONMENTAL JUSTICE**

#### **Chapter 4 - WSPA Support:**

First of all, members of our Association have long recognized and actively worked with many community groups and representatives on addressing environmental, health and safety impacts and reside near petroleum refineries as well as infrastructure facilities. As your staff has accurately noted, both the South Coast Air Quality Management District (SCAQMD) and Bay Area Air Quality Management District (BAAQMD) have active Environmental Justice (EJ) initiatives, policies, programs and outreach efforts to address concerns of the EJ community and their representatives. In fact, Cal/EPA and all its Boards, Directorates and Offices (BDOs) for the past few years have begun to implement EJ initiatives, policies and programs in each of their agencies. In particular, all the Cal/EPA BDOs have focused on ensuring public education and awareness and ensuring full public participation in all their decision-making activities

WSPA supports the fair treatment of people of all races, cultures, and incomes with respect to the development, adoption, implementation, and enforcement of environmental laws, regulations, and policies. We also support and seek opportunities to engage in an open dialogue with the local community and public agencies so that meaningful public participation takes place on issues relating to safety, public health and environmental impact.

As mentioned in the report, WSPA members are extremely active in the local communities in which they operate, providing significant contributions and in-kind support for school, civic and social service programs. It is also important to note that a significant number of petroleum industry employees, contractors and vendors live and work in many of the communities in which they operate.

We support the idea that the CEC should develop background materials on the state's need for petroleum infrastructure to provide all stakeholders with information useful in the decision-making processes.

Finally, we would like to point out that Cal-EPA is just now launching five comprehensive EJ pilot projects around the state to study and evaluate the environmental impacts of exposures as it relates to nearby communities.

WSPA is participating in these forums and is actively collaborating with the agencies in these efforts with the goal of addressing EJ issues.

#### **Chapter 4 - WSPA Concerns / Recommendations:**

***Ensure Development of Sound Science and Accurate Information:*** Although WSPA supports the need to develop tools that can be used to further community based efforts to address environmental and public health issues and concerns, it is important the tools that are developed, are based on scientific evidence and accurate information so that resources and efforts are focused on EJ issues of real concern.

***Demographic Analysis:*** WSPA also appreciates the demographic analysis conducted by staff of the population changes that have occurred between 1980 and 2000.

As noted in Tables 4-1 and 4-2 the dramatic changes and makeup of minorities and low-income populations in the years 1980 to 2000, indicate that certainly land use planning issues are important and necessary. The makeup of communities surrounding petroleum refineries and infrastructure facilities may have changed. However, we believe the report needs to emphasize that the demographic changes that have taken place around refineries, that were built largely in isolated areas many years ago, are likely an indicator of state and local policy implementation – especially zoning and is relative to affordable housing next to industrial facilities.

***Communities Located Near Refineries/Petroleum Infrastructure Facilities:*** We would also like to point out that living near a refinery is not an inherently negative experience. There are many areas that enjoy some of the lowest ambient air quality monitoring levels in the region and



therefore these communities do not receive a disproportionate impact from an air quality perspective. It should also be noted that the existing monitoring of refineries, including ambient air monitoring, contains some of the most state-of-the-art technology available today.

We understand that the CEC is currently considering co-funding a joint initiative with CARB to determine air quality impacts on minority and low-income communities. We welcome CEC's interest and efforts to work with other agencies on issues such as these. However, we would like to point out that Cal-EPA is already underway implementing five EJ Pilot projects statewide with the primary focus of reviewing environmental impacts on EJ communities. The agencies within Cal-EPA are taking respective leads on the five pilot projects.

We support Cal-EPA taking the lead on this issue, as they and their respective agencies have the necessary experience, knowledge and training to implement this project. On the other hand, we believe that the CEC should take an active role in ensuring the collaborative decisions on addressing EJ concerns also consider any regulatory impacts on supply. Ensuring Cal-EPA and its agencies understand the importance of balancing the need to address real EJ issues is an important role for CEC, in order to ensure current and future energy supplies can continue to meet the needs of California.

In that regard, we would like to point out one aspect that is not currently addressed in the report is the impact of EJ issues on refinery and terminal permitting.

Addressing EJ concerns can have a positive influence on the local community, although in some cases these issues can result in extending permit timelines, increased project costs, and might be a deterrent to in-state investment due to the uncertainty in permitting outcomes and timelines without commensurate environmental benefit.

### **Recommendations:**

- In the demographics section, WSPA recommends staff include additional language that indicates that not only are communities located near petroleum refineries and infrastructure concerned with environmental impacts on their health and safety, but that some communities enjoy some of the lowest ambient air quality monitoring levels in the region and therefore these communities do not receive a disproportionate impact from an air quality perspective
- While WSPA supports the CEC becoming involved in joint EJ projects with other agencies, we believe other agencies, such as Cal-EPA, are better equipped and more appropriate to take the lead on EJ issues, and not the CEC. However, we do urge the CEC to take an active role of ensuring the need for regulatory balance and the need to address EJ concerns, while also addressing the critical current and future energy needs for California.

#### **4. CHAPTER 5 – AIR QUALITY**

##### **Chapter 5 – WSPA Support:**

In general, WSPA supports the air quality and air regulations program in the State of California. We recognize and indeed support the interests of Californians who have, by tradition, led the way in the nation to improved air quality. It must be recognized that such historic improvements in air quality, since the 1960's and 1970's, has occurred despite nearly 10 fold increase in population and increases in population that are not diminishing. For example, currently, California is home to nearly 36 million Americans, which represents more than 12% of the U.S. population. This means that more than one in eight who live in the U.S. live in California. And this trend will continue as nearly 500,000 people (net in-migration) are added to the State's population each year. In 10 years, the prediction is that the State will add a population equivalent to those living in the Bay Area.

The CEC, as the State's energy agency needs to keep these facts in mind as they review the environmental programs in this state – because the petroleum industry has been able to reliably, safely, and economically provide energy to power the state while complying with the most stringent environmental regulations in the World. The industry produces the cleanest gasoline in the world and features the cleanest (lowest emitting) refineries in the World.

##### **Chapter 5 – Air Quality, WSPA Concerns / Recommendations:**

**Criteria air Pollutant Emissions:** On page 46, the EPR fails to place emissions from petroleum infrastructure in context for the reader. Petroleum infrastructure is believed to comprise less than 3% of criteria pollutant emissions in the air basins cited. In other words, despite providing nearly all the transportation fuels for the State, the petroleum industry only comprises, by CEC estimates, 3% of the emissions in the Bay Area and South Coast.

The need for context is more important than simply showing emissions. The CEC, and in fact agencies in general, need to keep in mind that the refineries in California represent approximately 10% of the Nation's refining capacity and produces gasoline, diesel, jet fuel and other petroleum products for all of California and parts of Arizona and Nevada. Our emissions, again by CEC estimates, are a small fraction of stationary source emissions, and an even smaller fraction of all emissions from mobile, stationary and area sources.

**Recommendation:** WSPA suggests the CEC add a table showing the percent of emissions from petroleum infrastructure compared to the total emissions in each air basin. Then insert a new table showing the emissions of the petroleum industry in terms of all California emissions (classified by stationary and mobile sources).

***Petroleum Sector Oxides of Sulfur Emissions:*** WSPA believes the “Bay Area Petroleum Infrastructure Emissions” of SO<sub>x</sub> in Figure 5-4 to be overstated. WSPA reviewed ARB’s web site<sup>1</sup> and calculated only 41.04 tpd for petroleum infrastructure sources. Please note, that WSPA believes even these estimates to be out of date and in need of review by the BAAQMD

**Recommendation:** We suggest CEC and ARB review data used for EPR for Bay Area emissions to ensure the most accurate data are reflected. We also suggest that a full review of the Bay Area Emissions inventory be initiated so that an accurate and current representation of Bay Area emissions be provided in the report.

Note also (p.65, 2nd paragraph), there is reference in the toxics section of the report to "methodological differences in the way various air districts derive emissions inventories result in data that are not directly comparable from district to district". Our comment cited here relates to BOTH criteria and non-criteria pollutants.

WSPA understands that one size (methodology) might not be appropriate for all Districts – and that some unique emission estimation techniques may be appropriate. However, given that emission inventory issues are more “technical” than policy, such unique applications should be rare. Instead, WSPA suggests that an emission inventory review process be initiated with interested air districts so that the best and most consistent data are developed. We feel this approach can be used for both criteria and toxic emissions – and that a consistent and science-based procedure will always render the best information.

***2002 Air Emission Footprint of the Four Petroleum Sectors:*** On page 51, the last paragraph states, "Oxides of sulfur emissions from refineries represent the largest tonnage of pollutants of the four sectors." Figures 5-8 through 5-10 do not necessarily support this finding. Only the Bay Area reports refinery SO<sub>x</sub> emissions higher than other pollutants.

**Recommendation:** WSPA recommends CEC delete this sentence or at the minimum correct the sentence. In terms of emissions of criteria pollutants, our understanding is the SO<sub>x</sub> is emitted in much smaller amounts, than perhaps NO<sub>x</sub>, VOC, or even CO. The comment, even if retained by CEC, argues strongly for a revisitation of the current emissions inventory.

***Future Trends:*** On page 55, the report states, “As shown in Figures 5-3 through 5-6, emission levels from the petroleum industry are expected be flat over the next 15 years with the exception of emissions increases in the Bay Area.” Unique in its emissions projections, BAAQMD projects emission increases for refineries based on increases in demand for petroleum products. In other words, BAAQMD assumes refining capacity will increase demand, while CEC predicts petroleum product imports will have to increase to meet demand.

Both agencies cannot be right. Given that the petroleum industry is constrained by current federal and state permit limits, the CEC statements seem particularly odd. CEC should either delete the statement or clearly state the reasons why it believes emissions from refineries will

---

<sup>1</sup> [http://www.arb.ca.gov/app/emssumcat\\_query.php?F\\_YR=2004&F\\_DIV=-4&F\\_SEASON=A&SP=2005&F\\_AREA=DIS&F\\_DIS=BA](http://www.arb.ca.gov/app/emssumcat_query.php?F_YR=2004&F_DIV=-4&F_SEASON=A&SP=2005&F_AREA=DIS&F_DIS=BA)

increase in the Bay Area. Any such assertion by CEC must consider existing state and federal permit limits that are currently enforced on refineries, the historic reductions in emissions from refineries through time, and the rather limited opportunity for permitting of new emission sources within refineries.

Again on page 55, WSPA disagrees with the statement:

*“Continued reformulations of diesel to low and ultra-low sulfur levels will reduce ambient levels of SO<sub>2</sub> from the transportation sector, but will require lower sulfur crude oil feedstock or enhanced sulfur removal equipment at the refineries. Increasing sulfur removal from the refined products at the refineries could increase SO<sub>2</sub> emissions unless SO<sub>2</sub> emissions controls at the refineries are also improved.”*

The last statement is particularly curious. While there may be some merit in the reductions of sulfur in fuels, this does not necessarily mean that SO<sub>x</sub> emissions will also increase. Such emissions can only be allowed by permit.

The CEC should revise the statement to read “Continued reformulations of diesel to low and ultra-low sulfur levels will reduce ambient levels of SO<sub>2</sub> from the transportation sector, and could require lower sulfur crude oil feedstock or enhanced sulfur removal equipment at the refineries. Increasing sulfur removal from the refined products at the refineries is not expected to increase SO<sub>2</sub> emissions from refineries”.

***Percent Contribution of Petroleum Infrastructure to District Emission Inventories, Table 5-4:***

On page 56, WSPA calculates the Bay Area percentage of SO<sub>2</sub> emissions as 57.3%. Again this argues for revisitation of the BAAQMD inventory.

**Recommendation:** See page 18 comments on Bay Area SO<sub>x</sub> emissions.

***Environmental Concerns: Refineries – Flaring and Air Quality Monitoring:*** On page 59, the third paragraph states, “Obtaining real-time ambient air monitoring data is important when investigating routine, non-routine, and upset conditions that may occur at a refinery. Real-time data can indicate whether unusual levels of pollutants detected may have a public health impact.”

We agree that improved monitoring using proven technology can provide valuable information that can indicate areas of process improvement. However, in order to educate the public, the CEC should differentiate between the many types of monitoring and the benefits of such procedures. For example, ambient monitoring (measurement of ambient air quality for criteria pollutants and toxics) is valuable because it gives the public an understanding of the quality of air they breathe.

But such monitoring does not, and cannot, reveal the sources of pollutants that might be found, nor can ambient monitoring determine the impact of emissions, exposure, or risk.

Conversely, source (emissions monitoring) can determine with some assurance, the emissions that are released from various monitored sources. But such emissions cannot with any degree of

reliability indicate environmental or community impact due to natural dispersion or dilution. In addition emissions from small/unregulated sources can be a contributing factor to environmental impacts. Finally, as stated earlier, source emissions do not reflect in any real sense, exposure, dose or risk. In other words, neither source monitoring nor ambient monitoring can by themselves indicate risk or potential health impacts.

**Flaring:** The CEC report appears to provide an incomplete view of refinery flaring systems and the emissions from those systems. Flare systems are first and foremost a safety system designed to safely combust gases and relieve system over-pressures. Flaring events are intended to destroy gases that might otherwise escape to the environment – so in that sense, flares REDUCE emissions of unwanted substances to the environment.

In the Future Trends section of the Toxics section (P. 69), the CEC references the fact that emissions from flaring have declined and will likely decline further as air district rules are implemented. WSPA agrees that flare emissions (and events) have diminished through time – and it is clear that emissions will continue to be reduced as refineries implement process improvements and Best Management Practices. Another reason for the reduction is that the flare emissions inventory might have been unreasonably high due to very conservative emission estimation techniques, which would be substituted by improved monitoring and CEM data. Hence, improved data measurement can, by itself, lead to reductions in the emission inventory.

**Recommendations:** WSPA recommends the following comments be incorporated into the Flaring section of the EPR:

- Refinery flares are first, and foremost, essential safety devices. It is also important to note, the use of flare systems to safely control refinery vent gases is already required by several Air Quality Management Districts and federal rules.
- The EPR should also note that flare emission reductions have already been achieved through equipment modifications, implementation of improved flare management practices and other facility improvements appropriate for each refinery's specific operations and design
- Refineries have worked hard to reduce emissions from flaring. In fact, the SCAQMD have reduced emissions by over 80 percent since monitoring and measuring was initiated. This reduction has already brought emissions to a level of 1.2 tons/day, which is well below the level of 2.2 tons/day, as required by the SCAQMD's State Implementation Plan (SIP) – it should also be noted that this reduction has been achieved a full 5 years in advance of the deadline date of 2010!
- In addition, since installation of state-of-the-art monitoring equipment in the Bay Area in 2003, it has been determined that flares contribute less than 1/1000<sup>th</sup> of the region's smog-forming emissions.

**Staff Findings and Policy Options:** On page 61, in the first bullet on this page CEC staff recommends “Refinery upgrades of leak-detection and repairs, and implementation of programs to minimize the number and severity of flaring events.

With respect to leak detection and repair (LDAR), such programs at California’s refineries are the most stringent in the Country. Every valve, connector, flange, tank seal, and vent is routinely inspected for leaks and repaired based on a strict mandated schedule. There are no feasible emission reductions available from these sources due to the effectiveness of these state-of-the-art programs.

In fact, in 2004 BAAQMD adopted revisions to its Regulation 8 Rule 8: Equipment Leaks. The BAAQMD staff report for this rule amendment states, “...*there has been a general downward trend to fugitive emissions over the last several years. This trend is largely due to improvement in the leak detection and repair programs over time.*” The inventory for all valves, pumps, compressors, pressure relief devices, and connections is reflected as 2.32 tpd. This same situation holds true for refineries in the South Coast as well. Any incremental increase in stringency of control measures, in the face of already stringent regulations, would gain only marginal emission reductions.

#### **Recommendation:**

The CEC needs to substantially rewrite and clarify several statements. WSPA recommends the following sections be reviewed and revised as noted below:

- On page 65, the 1<sup>st</sup> paragraph states that air toxics do not have associated federal or state ambient air quality standards specifying levels that are safe to breathe. This statement, while true, might give the reader a misconception. The CEC should in all fairness report on the extensive federal, state and local regulations that govern emissions of toxic air contaminants.

In other words, while there are few ambient air quality standards for toxics air contaminants, federal, state and local regulators have concentrated on reducing emissions from such unwanted compounds – rather than trying to find out what’s “safe”. Hence, all levels of government look at both emissions and release inventories for such compounds as part of the EPA Tri-annual (TRI) report, the State AB 2588 (Tanner/Toxic Air Contaminant) process, CUPA process, AB 3777 (risk management process), and then a myriad of local (AQMD/APCD) regulations limiting the release of toxic air contaminants. Certainly, the CEC should consult the SCAQMD Rule 1401, and Rule 1402 and Bay Area Regulation 2, Rule 5.

- On page 65, 6th paragraph, it states that in Ventura and Santa Barbara County's, "diesel PM emissions from ocean going ships transporting crude oil and petroleum products account for almost 30 and 60% of total diesel PM emissions"

This statement on the surface seems curious since the Santa Barbara County Air Pollution Control District (SBCAPCD) states in its' OCS 2004 Emissions Inventory for NOx that petroleum tankering makes up only 3 % of the total OCS emissions inventory, while container ships make up 84 % of the NOx emissions. Also, according to study conducted by the SBCAPCD, of all the ocean-going vessel transits, petroleum tankering transits make up only 7 % of the annual total.

WSPA also contacted the Ventura County Air Pollution Control District (VCAPCD) and was informed the VCAPCD derived all their emissions inventory data for offshore marine vessel activity on SBCAPCD data.

Based on this information, WSPA believes the CEC has confused petroleum tankering diesel PM emission data with container ship data. For further information on Marine Vessel Emissions, see Appendix 2, which contains a study that was conducted by the Santa Barbara APCD and identifies the emission inventory and contributions of emissions from ocean-going vessel transits compared to petroleum tankering transits.

- On page 66, in the Sources of Toxic Air Contaminants section, CEC states: "...only benzene and diesel PM are among the seven air toxics emitted in the greatest quantity from petroleum infrastructure facilities".

The industry is proud of its environmental practices and its success in reducing emissions of toxic emissions. As CEC notes, the petroleum infrastructure is responsible for only two of the most ubiquitous compounds based on emission inventories. While emissions of benzene have been reduced to nominal concentrations due to process controls and reformulation, diesel PM emissions from trucks used in commerce and industry have been increasing. However, new technologies and expanded use of Ultra Low Sulfur Diesel are expected to reduce emissions from diesel engines.

- On page 69, in the Future Trends section, CEC references the fact that emissions from flaring have declined and will likely decline further. We agree – and believe that the CEC is correct in stating that emissions will diminish. As the industry reviews BMPs, and operations improvements, emissions may be reduced to a minimum around which they fluctuate year to year due to emissions from shutdowns and turnarounds. It should be clear also that the initial emissions inventory attributed to flares and flare usage might have been wrong (elevated) to begin with – making the trend in reduced emissions even more noticeable. The best science available indicates flares combust at least 98% of all organic compounds (including toxics) entering the flame
- On page 70, in the Environmental Concerns section, CEC states that diesel PM from shipping activities associated with marine terminals account for over 99% of diesel PM from "petroleum infrastructure sector". The CEC statement does not appear to be substantiated by documentation. It is not clear what emissions the CEC is including within the marine terminals (ship emissions in transit? Ship emissions at the terminal? )

Nor is it entirely clear what the CEC has defined petroleum infrastructure to include. At the very least, CEC should provide documentation for its statements.

- On page 70, last paragraph, CEC references that the 2 air districts "recognized that flaring is a significant source of air toxic emissions. This statement needs to be withdrawn or totally rewritten because it is clearly wrong. Flare systems combust gases and other compounds that should not be released to the environment. In fact, flaring is a known control measure to reduce toxic air emissions. Hence, as a safety device, such systems are designed to reduce emissions of air toxic emissions to the lowest technically feasible concentrations.

## **5. CHAPTER 6 - PUBLIC HEALTH IMPACTS OF TOXIC POLLUTANTS**

### **Chapter 6 – Findings and Policy Options Section - WSPA Support:**

WSPA supports certain aspects of staff's Findings and Policy Options section. Specifically, we support the finding, based on CARB data that air monitoring studies did not identify significant health risks associated with refineries in Crocket<sup>2</sup> (Northern California) and Wilmington (Southern California).

Additionally, with the exception of staff's claim that diesel particulate matter emissions from marine shipping and port facilities, WSPA supports the following conclusions on the public health impacts of toxic pollutant from petroleum infrastructure:

- No acute hazards
- No identification of significant health risk associated with refineries
- Recognition that emissions from flaring have declined and continued to decline
- Air Toxics do not exceed regulatory risk
- Except for diesel emissions and emissions from marine shipping and port activities, air toxics from normal operations of petroleum infrastructure are not a major contributor to public health risk.
- No significant cancer or non-cancer risk associated with normal operation

### **Chapter 6 – Findings and Policy Options Section - WSPA Support:**

***Recommend Re-organize Chapter 6:*** Generally speaking, WSPA recommend staff consider re-organizing Chapter 6 into a format so that the reader clearly understands the history and regulatory requirements by federal, state and local agencies in addressing health impacts from toxic pollutants.



**Concerns with Certain Statements:** WSPA is concerned with certain statements that may confuse the reader or result in additional concerns that were unintended. Listed below are some examples of our concerns and suggested recommendations:

- ***Air Toxic Pollutants:***

On Page 65: 1<sup>st</sup> paragraph, staff stated the following:

“Unlike criteria air pollutants such as NO<sub>x</sub> (see the Air Quality section), air toxics do not have associated federal or state ambient air quality standards specifying levels that are safe to breathe”.

WSPA is concerned that the above statement may imply that air toxic emissions from petroleum infrastructure facilities are not safe to breathe. This is not true. In fact, federal, state and local agencies have been developing and implementing air toxic programs, regulations, rules and controls for the past 25 years. Specific programs include, the federal National Emission Standards for Hazardous Air Pollutants (NESHAPs), which include standards for air toxic pollutants as such benzene. Also, as noted in the staff report, CARB, in association with the Office of Environmental Health Hazard and Assessment (OEHHA) department, has been in the forefront of leading the nation in the identification, review, analysis and development of unit risk factors and hazard index levels for toxic air contaminants (TACs).

Additionally, air districts in California have for many years implemented air toxic regulatory programs and rules to review, analyze and limit the release of TACs. Many air districts, including the South Coast AQMD and BAAQMD, already have strict permitting and risk standards that facilities must comply with when obtaining necessary permits when building, modifying or expanding petroleum infrastructure operations.

**Recommendation:** WSPA recommends the staff include reference of the above regulatory and permitting requirements in this section so that the reader understands the stringent air toxic emission standards and controls the petroleum industry is required to meet. The CEC should also collaborate with CARB on the significant reductions in TACs achieved since 1996.

- ***AB 2588 Air Toxic Hot Spots Program:***

On Page 65: 5<sup>th</sup> Paragraph, the report states the following:

"In all air districts, petroleum infrastructure facilities account for less than three percent of emissions of benzene, which is the third highest-risk air toxic in California."

**Recommendation:** WSPA recommends adding the following statement in the above section:

"No refinery or surrounding community is designated as a "Toxic Hot Spot" under AB-2588."

- ***Diesel Particulate Matter and Benzene Emissions:***

On Page 66, the report states the following: "Of the ten air toxics listed in Table 6-1, only benzene and diesel particulate matter are among the seven air toxics emitted in the greatest quantity from petroleum infrastructure facilities." While the next sentence puts the emissions in context, this sentence is inaccurate. None of the refineries in California contribute more than minimally to benzene and PM emissions.

**Recommendation:** WSPA recommends the following sentence should be included in this section:

*"Increases in toxics emissions at stationary sources are restricted by Toxics New Source Review which limit emissions of carcinogenic compounds to less than 10 in a million which is LESS risk than posed by ambient air."*

- ***Emission Upsets from Petroleum Facilities:***

On Page 70, the report states, "Emissions from upsets at petroleum facilities have the potential to be significant compared to routine emissions." Because of efficient flare combustion and the fact most surviving compounds will be dispersed high in the atmosphere, ground level monitoring has rarely exceeded health-based standards. For example, the Contra Costa County Health Services Department, which has a sophisticated community warning, response, and monitoring system for such events has indicated NO adverse health impacts from upsets in the last five years.

## **6. CHAPTER 7 - SAFETY AND HAZARDOUS MATERIALS MANAGEMENT**

### **Chapter 7 - WSPA Supports:**

WSPA would like to acknowledge that CEC staff basically captured the industry's generally outstanding safety record and the industry's continuing efforts to reduce accidental releases of hazardous material and to reduce exposures and risks.

In particular the report analysis of 18 incidents from the National Release Centers Incident Reporting System (IRIS) database that had the potential to impact the public, identified that none of the 18 were found to have injured any member of the off-site public and highlighted that industry commitment to safeguard the public around our facilities.

Staff's conclusion that the petroleum industry is doing a good job of protecting the public from impacts resulting from accidental releases of hazardous materials further points to the industry's generally outstanding hazardous material safety record. .

Further, WSPA would like to support staff's contention "that there will be an overall trend toward continued reduction in risk of impacts to the public as a result of petroleum processing..." The industry is committed to Process Safety Management, Risk Management

Planning, Offsite Consequence Analysis and Homeland Security assurance. All these efforts will lead to improved safeguards to the public around our facilities. We believe that reductions in worker injuries and off-site impacts over the last 20-years, concurrent with increased demand for use of our products, also reflects the industry's commitment to safety improvements and risk reductions.

## **Chapter 7 – Safety and Hazardous Materials Management:**

### **WSPA Concerns / Recommendations:**

WSPA is concerned with the apparent conflicting messages that exist in the report. On the one hand, CEC concludes that petroleum has a good record of managing potential risk of public exposure associated with use of hazardous materials, but on the other hand claims that existing hazardous regulations may not be adequate to address future challenges. California's refineries are already some of the most complex, sophisticated refineries in the world producing over 18 billion gallons of fuel annually. We fully expect that as the refineries become even more sophisticated, they will continue to meet the challenge of protecting the neighboring public.

WSPA acknowledges that industry, hazardous material regulators, safety regulators, emergency responders and security agents must continue to be vigilant and strive for continuing improvement. However, as stated on Page 7 above, WSPA members take very seriously the issue of safety and protection against terrorist threats, and WSPA members in association with the American Petroleum Institute (API) has been on the forefront of developing security guidelines for the petroleum industry. Additionally, as mentioned previously, WSPA is working closely with the US Coast Guard and the Department of Interior, Minerals Management Services on developing and implementing regulations on safety and security for pacific offshore platform safety zones.

The CEC should recognize that efforts to improve coordination among all these agencies and with industry are happening now. Our facilities work on a daily basis with firefighters, emergency responders, safety and security agencies. Coordination is improving and will continue to improve. We acknowledge that the regulatory scheme is complex, but it is also comprehensive. CEC staff could be well served to more fully understand how the public is protected under the existing regulatory framework.

**Recommendation:** WSPA recommends staff review this section and incorporate by reference the safety and security guidelines developed by API as well as the on-going activities by other agencies such as the U.S. Coast Guard and Department of Interior efforts. We also recommend the EPR reference the coordination between emergency responders, safety and security programs and the integration with facility firefighters and County and City Emergency agencies.

## **7. CHAPTER 8 - HAZARDOUS WASTE GENERATION AND MANAGEMENT**

### **Chapter 8 - WSPA Support:**

WSPA supports staff's finding that opportunities exist for government and industry to jointly work on evaluating and incorporating new approaches to waste management.

In fact, WSPA and its member companies work jointly with DTSC to sponsor yearly Petroleum Industry Pollution Prevention Symposia where ideas are freely discussed on how everyone can do a better job of managing hazardous waste.

WSPA also noted and support staff's finding that the threat to groundwater from releases at refineries has been minimal as a result of new practices and technologies and that the majority of releases reported in recent years less than 50 gallons. For example, our companies have systematically upgraded tankage with improved bottoms and daylighted refinery pipes to reduce undetected leaks. When combined with increased inspections, monitoring, audits, improved safety procedures and personnel training leaks and releases have been greatly controlled.

Finally, WSPA does agree that we should work with the DTSC to expand energy efficiency related to waste products - zero waste and maximal energy efficiency are certainly goals to work toward, however, it is important to note that the petroleum industry has accomplished a great deal in the area of hazardous waste generation, management and reduction.

### **Chapter 8 – Hazardous Waste Generation and Management**

#### **WSPA Concerns / Recommendations:**

Despite our support of some of the issues staff raised, we are concerned that the whole Chapter was somewhat fragmented in the information it reported and some of the findings. We are disturbed the report concludes that, "*Data on hazardous waste generation and management are inconsistent and often lacking for petroleum infrastructure facilities.*" That premise is then followed by a discussion of the elaborate regulatory framework and stringent requirements that exist and how California has even more strict and effective enforcement than the federal requirements.

Additionally, we believe the Report needs to clarify which petroleum facilities are actually being referenced in this chapter. Is the information and concerns expressed by staff related to upstream, pipeline, refining or marketing facilities?

First and foremost, our companies fully cooperate and partner with DTSC, CUPAs and other agencies to ensure that hazardous waste management and reporting is meeting the letter and spirit of both the federal and state regulations. Our companies are very proud of their achievements in hazardous waste management and reduction.

Your report highlights a 45% reduction in hazardous waste generation since 1990. But we should add that the petroleum industry was a leader in the implementation of the SB 14 source reduction program, which has a baseline year of 1986. Our reductions since 1986 are much, much higher-- we estimate over 75%.

We also respectfully disagree that 5% of the total manifested waste or that 7-16% of the landfill waste is a "major" share of the state's hazardous waste. It must be remembered that in California, we have what is called "California-only" hazardous waste. Our facilities must manage significant volume of wastes (especially soils) that are not hazardous anywhere else in the country.

Finally, we were surprised see a statement that there is inadequate data on hazardous waste generation, remediation and reduction. There has been so much progress on hazardous waste management that is not reflected in this Section. We would highly recommend the CEC staff consult more closely with Cal-EPA DTSC to gain a more thorough understanding of the strict regulations that govern hazardous waste management from "cradle to grave" not just on the petroleum industry but all industries. This Section of the EPR does not leave you with that impression.

**Recommendations:** WSPA recommends staff contact the DTSC regarding the extensive hazardous waste management program they implement and the regulatory requirements the petroleum industry is required to comply with in the handling, transportation and disposal of hazardous waste materials. WSPA would be happy to help facilitate a meeting with the DTSC on this issue.

## **8. CHAPTER 9 - WATER QUALITY AND SUPPLY**

In general, we agree with most of statements in Chapter 9. We appreciate the CEC's recognition of the high level of existing water-related regulatory requirements on our industry. The EPR does a good job of itemizing the new technology that is being used to prevent spills, and then notes that over 90% of spills in a twenty-year period were less than 100 gallons.

However, we do question the statement that: "... water use by petroleum industry does not appear to be subject to any formal oversight at this time." Our facilities in the late 1980's and early 1990's invested significant sums in reducing process water use – and in fact we use large amounts of recycled industrial water. The NPDES system that all facilities have in place strictly regulates discharges and looks very closely at the volumes of water that are discharged. We would be happy to examine the need with the CEC on whether or not petroleum would benefit from a water -use efficiency review as the report suggested and understand this will be further discussed as part of the CEC's June 2005 Water- Energy Relationship Report June 2005.

## 9. CHAPTER 10 – BIOLOGICAL RESOURCES

### Chapter 10 - WSPA Support:

Despite the fact that Chapter 10 attempts to cover a wide range of issues and topics, WSPA is pleased that staff acknowledged the WSPA members extensive record in protecting biological resources. Also, the report states our industry is complying at nearly 100% with regulations. Clearly information such as this reflects how seriously WSPA members take its responsibility of ensuring the transportation and handling of petroleum and petroleum products. Further, it is this track record that we believe supports our position, which is why we do not agree with a statement that increases in shipping petroleum products into CA will have increased detrimental effects.

### Chapter 10 – Biological Resources, WSPA Concerns and Recommendations:

There are a number of inaccuracies that we believe need to be addressed, our concerns are as follows:

***Federal Ballast Program, Page 105:*** In the second paragraph, EPA infers that there is no federal ballast water program, which is incorrect. Starting in November, 2004, the U.S. Coast Guard (U.S.C.G.) started ballast water compliance inspections. Several thousand vessels have been boarded and inspected for compliance with ballast water exchange requirements. Also new federal ballast water legislation is being proposed and is working its way through the legislature.

**Recommendation:** WSPA recommends the staff revise this section of the EPR and reference the U.S.C.G. ballast water compliance inspection program.

***Vessel Size, Page 108:*** The last paragraph states: “*As vessel size increases... ..the transport of Non-indigenous aquatic species (NAS) in the ballast water can be increased.*” We do not know how staff determined that increased vessel sizes automatically increases water ballast, when in fact, the newer vessels are being built to comply with open water ballast exchange requirements.

**Recommendation:** WSPA recommends staff revise this section of the EPR to reflect that newer vessels being designed and built to comply with open water ballast exchange requirements.

***Ballast Water, Page 109:*** WSPA is concerned that the first sentence on Page 109 is incorrect or at a minimum is mis-leading to the reader. In fact, ballast water is taken on while at the unloading port and ballast water is discharged at the loading port.

Also, the fourth paragraph references “New technologies” to help remove or inactivate NAS are currently under development as well as land based treatment technologies may also be possible for treating ballast water.

While we are clearly interested in ways to address concerns of NAS, none of the technologies referenced to date in the EPR have been developed and approved for use. Although there are numerous companies working to develop ballast water treatment, at this time, proposed treatment technologies all have issues associated with them. For example, some of the technologies may work for small volume discharges such as Cruise Ship but will not work for tankers with large volumes. Alaska Tanker Company installed and tested an ozone injection system that had unsuccessful kill rates. Additionally, biocides and chlorine treatment are currently being evaluated, however, there is an issue of concern associated with the environmental impact of discharging these biocides into receiving waters.

Additionally, staff referenced a ballast water treatment facility located at the Alyeska Terminal in Prince William Sound, Alaska. We would like to point out that the referenced facility in Valdez is not for NAS treatment, but is for cleaning up oily ballast water only.

**Recommendation:** WSPA recommends staff clarify the Ballast Water and Nonindigenous Aquatic Species section to reflect that ballast water is taken on at the “unloading port” and discharged at the “loading port”. Further, WSPA recommends this section be revised to reflect the fact that new technologies are currently under review, however, there are environmental issues and challenges associated with their use as possible ways to inactivate NAS.

**Page 110:** We support staff’s statement that the amount of oil spilled in recent years has been reduced, however, the statement that: “The majority of spills in California are from crude product in pipelines”, needs to be clarified to be crude oil – petroleum products – or both.

**Petroleum Seeps, Pg. 111:** The section on Offshore Oil Spills references “petroleum seeps” that can have on-going long-term impacts and if the oil from seeps reach shore, can substantially impact the intertidal ecosystems. WSPA believes when staff states “petroleum seeps” they are referring to “natural seeps” and the statements regarding impacts to the ecosystems are incorrect. The natural seeps have been producing oil on the beach for centuries and is part of the ecosystem in those geographic areas.

To underscore this point, it is important to note that the second largest concentration of natural seeps of both gas and crude oil in the world are located in the Santa Barbara Channel. It has been estimated that over 1.8 million barrels of oil have seeped naturally from this location since 1970 alone. Daily averages of approximately 6,000 barrels of oil and 5 million cubic feet of gas naturally seep there everyday

**Recommendation:** WSPA recommends staff revise the section on “petroleum seeps” the include and clarify that natural petroleum seeps have been producing oil on the beach for centuries and is part of the natural ecosystem.

**Future Trends Section, Pg. 114:** In the Future Trends section the first paragraph incorrectly assumes that as imports of petroleum products increase, so will the risk of oil spills and ongoing need for maintenance of facilities and waterways.

We recommend staff to clarify their statements on this fact and provide information to support their assumption of the increased risk of oil spills as a result of increased importation of petroleum products.

Further, we believe the second paragraph regarding ballast water is confusing in that it states that water introduction of NAS has become an increasing problem, yet references the fact that industry compliance with existing ballast water regulations is close to “100 percent”.

**Recommendation:** WSPA urges staff to review this section and clarify to the reader the fact that compliance is literally universal and as increased efforts are made to address ballast water, concerns with NAS issues will decline.

**Dredging:** WSPA is concerned that the section on Dredging (page 99) fails to highlight some of the benefits dredging activities can bring to the SF Bay, namely the reuse of clean dredge materials to build, rebuild and restore wetlands in the SF Bay region. Restoring wetlands is consistent and in accordance with the SF Bay Long Term Management Strategy (LTMS) for the placement of dredged materials in areas that have experience subsidence and loss of wildlife habitat (“Long Term Management Strategy for the Placement of Dredged Material in the SF Bay Region, 2001”). The ability to reuse dredged materials has generated interest by the EPA Region IX, BCDC, Army Corp. of Engineers, USFWS, and the SF RWQCB, who are member agencies to the LTMS. Several agencies have seen the value of utilizing the ecological benefit of restoring wetlands and wildlife habitat through the use of dredged materials and we believe this beneficial use outweighs the concerns over sedimentation considering the 2.5 million kg/yr inflow of sediment to the Bay from the Delta and local tributaries (Mercury in the San Francisco Bay: Total Maximum Daily Load, April 2004).

**Recommendation:** WSPA requests an additional paragraph for insertion at the top of pg. 110, that would provide balance and a more accurate depiction of how dredging relates to Biological Resources:

*“Dredge materials from SF Bay are being used in part for the restoration of wetlands and wildlife habitat. The LTMS (Long Term Management Strategy) for the beneficial reuse of dredge material, supported by EPA IX, BCDC, Army Corp. of Engineers, USFWS, and the SF RWQCB documents the importance of dredge materials for this purpose. Considering the diverse and populated biological communities in SF Bay, along with the 2.5 million kg/yr sediment influx from the Delta and local tributaries, it is not clear that increased dredging would measurably amplify sedimentation or impact biological communities”.*



# **The Need to Reduce Marine Shipping Emissions: A Santa Barbara County Case Study**

**Paper # 70055**

**Tom M. Murphy**

Planning and Technology Supervisor  
Santa Barbara County APCD  
26 Castilian Drive, Goleta, CA 93117

**Ray D. McCaffrey**

Air Quality Engineer III  
Santa Barbara County APCD  
26 Castilian Drive, Goleta, CA 93117

**Kathy A. Patton**

Technology and Environmental Assessment Division Manager  
Santa Barbara County APCD  
26 Castilian Drive, Goleta, CA 93117

**Douglas W. Allard**

Air Pollution Control Officer  
Santa Barbara County APCD  
26 Castilian Drive, Goleta, CA 93117

## **ABSTRACT**

Marine shipping, the largest unregulated source of oxides of nitrogen (NO<sub>x</sub>) emissions, represents a significant long-term obstacle to achieving ozone standards in coastal areas, as documented in the example of Santa Barbara County in California.

According to the Santa Barbara County Air Pollution Control District (APCD) 2001 Clean Air Plan, 1999 base year NO<sub>x</sub> emissions from marine vessels were more than those from all on-road motor vehicles, and comprised just over a third of the total NO<sub>x</sub> emissions inventory. By 2015, the Plan projects that NO<sub>x</sub> emissions from ships will be almost five times greater than those from on-road motor vehicles, and comprise more than 60 percent of the total NO<sub>x</sub> emissions inventory.

The projected increase in marine shipping emissions essentially negates all the NO<sub>x</sub> emissions reductions expected to occur onshore, and brings the 2015 inventory to levels close to those experienced in 1999, the year Santa Barbara County attained the federal one-hour ozone standard. This jeopardizes the county's ability to maintain the ozone standard. Achieving reductions in marine shipping emissions is critically important for the county's long-term air quality, especially as it is increasingly difficult to obtain cost-effective onshore emission reductions.

Since more than ninety percent of the NOx emissions from vessels transiting offshore the county fly foreign flags, and the existing fleet has a slow rate of turnover, the task of reducing marine shipping emissions is a challenging one. While regulatory approaches may achieve NOx emission reductions over the long term (10-30 years), incentive programs and partnerships to reduce emissions from existing vessels are essential for continued air quality improvements in the near term (1-10 years).

This paper provides information about the Santa Barbara County emissions inventories, places this information in a national and international context, outlines the existing regulatory framework, identifies opportunities for near-term cost-effective emission reductions, and highlights the need for incentives and partnerships to gain momentum in reducing marine shipping emissions through demonstration programs. Much of what we have learned and will present is thanks to the work of others who have been researching this issue for many years. And while this paper presents Santa Barbara County specific data, we believe that the information is germane to other areas of the nation and internationally.

## INTRODUCTION

There is a growing awareness internationally of the significance of shipping emissions. Ships are increasing in number, size, carrying capacity and speed, while fuel use is increasing proportionally.<sup>1,2,3,4</sup> In addition, residual heavy fuel oil – the most common fuel used in large ship engines – is decreasing in quality, while a greater number of engines are being designed to use this lower-quality fuel.<sup>5</sup>

There is also an increasing awareness of the impacts of shipping emissions on onshore air quality. An estimated 85 percent of international shipping traffic occurs in the northern hemisphere, and 70 percent of that is within 400 km (240 miles) of land.<sup>6</sup> Much of the shipping activity and associated emissions occur near major urban areas, many of which are already struggling with air quality problems.

There is a range of estimates for NOx emissions from marine shipping activities. The United States Environmental Protection Agency (USEPA) estimates that approximately 4.4 percent of total NOx emissions in the United States come from compression ignition marine engines.<sup>7</sup> One study estimates that NOx emissions from US ships are 127,000 tons/year (inland rivers) and 317,000 tons/year (ocean-going).<sup>8</sup> According to a study conducted for USEPA in 1991, ocean-going marine vessel emissions contributed more than 11 tons per day of NOx in New York/New Jersey and 19 tons per day of NOx in the Houston/Galveston area.<sup>9</sup> A recent estimate of year 2000 NOx emissions from ocean-going vessels in the Vancouver, B.C. region is close to 15 tons per day of NOx.<sup>10</sup> NOx emissions from ocean-going ships in the South Coast Air Basin for the year 2000 are estimated at 35 tons per day.<sup>11</sup>

Santa Barbara County is situated on the west coast of California between San Luis Obispo County to the north and Ventura County to the east. Even though Santa Barbara County does not have a port, more than 33 tons per day of NOx were produced by marine

shipping activities offshore the county in 2000 – a figure more comparable to those estimated for Los Angeles and San Francisco. This is due to several factors. There is a very high volume of vessels transiting along the Santa Barbara County coastline, and most of these vessels use large, higher polluting, two-stroke engines. The county also has 130 miles of coastline, so these vessels are traversing a relatively long distance. In addition, much of the emissions associated with shipping activities occur between 10 to 20 miles from shore, as ships traverse the California coastline and/or use great circle routes throughout the Pacific Rim.

Santa Barbara County is currently classified by USEPA as a “serious” nonattainment area for the federal 1-hour ozone standard but has applied for redesignation as an attainment area. APCD developed a 2001 Clean Air Plan to support the application for redesignation, and to demonstrate continued attainment of the 1-hour standard for at least 10 years after redesignation.<sup>12</sup>

Based on accepted methodologies for estimating marine vessel emissions, primarily as detailed in the 1999 ARCADIS emissions inventory report,<sup>13</sup> inventories developed for Santa Barbara County’s 2001 Clean Air Plan showed that marine shipping emissions represented approximately one-third of estimated NOx emissions for 1999. Marine shipping was thus the single largest source of NOx emissions, contributing an amount comparable to the NOx emissions from all trucks, cars, and buses operating onshore. In the 2015 emissions forecast, marine shipping emissions represent more than 60 percent of NOx emissions and are almost five times greater than those from on-road motor vehicles. The dramatic increase in NOx emissions from this source through the planning horizon essentially negates anticipated NOx reductions onshore from local, state and federal air programs. This also jeopardizes APCD’s ability to show continued attainment of the federal 1-hour standard through 2015.

Data collected to calculate marine shipping emissions offshore Santa Barbara County during 2000 reveal several specific points of interest:<sup>14</sup>

- 6,424 total transits occurred offshore the county (an average of almost 18 transits every day of the year)
- 1,363 different individual vessels transited the coastline
- 91 percent of the emissions were from foreign-flagged vessels
- 10 percent of the individual vessels contributed 50% of the emissions
- 44 of the vessels each emitted more than 50 tons per year of NOx.

In Santa Barbara, we have assigned the moniker “frequent flyers” to those vessels that create the most emissions each year, due to a combination of the emissions characteristics of their engines, the fuel they burn, and the number of transits they make each year. One very interesting feature is that 10 percent of the ships make up 50 percent of the marine shipping emissions offshore Santa Barbara. The fact that a relatively small number of ships contributes a large percentage of emissions provides a unique opportunity to obtain significant emission reductions with retrofit technologies.

Efforts to regulate the emissions from marine shipping have been largely ineffective to date. More stringent regulations, and a more intensive focus on international implementation, are needed to encourage the development of engines that will be substantially cleaner than those already on the market today.

While regulatory efforts are of critical importance to reducing emissions in the long term, near-term strategies must also be pursued. The California Air Resources Board (CARB) has initiated the Maritime Working Group to provide a forum for discussion of air quality issues and concerns pertaining to maritime activities in California. This group draws upon a large group of interested parties including USEPA, local California air districts, port representatives, ship owner/operators, the Maritime Administration, engine manufacturers and emission control technology providers. Preliminary estimates indicate that implementing retrofit emission control technologies on existing ocean-going vessels could provide very cost-effective emission reductions relative to those already implemented onshore. The status of current efforts to reduce emissions from the existing vessels, and the need to continue to build partnerships to address this large source of emissions, will be discussed in this paper.

## **MARINE SHIPPING EMISSIONS INVENTORY**

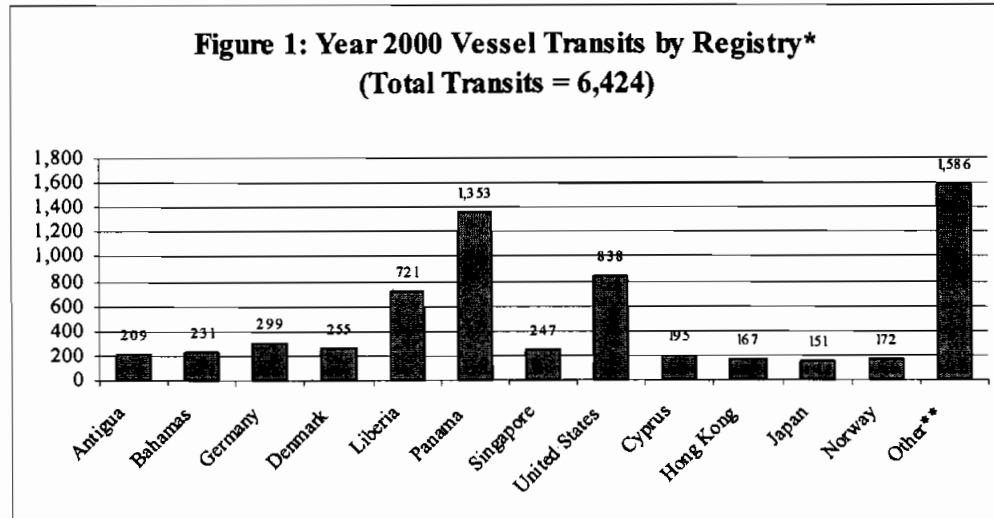
The NO<sub>x</sub> emissions from marine shipping activities offshore Santa Barbara County are largely due to three principal factors:

- There is a high volume of transits along the Santa Barbara County coastline.
- The majority of the vessels use large, higher polluting, two-stroke engines.
- The county has 130 miles of coastline, so these vessels are traversing a relative long distance. Much of this travel is through the Santa Barbara Channel, which is only 10-20 miles from the shore.

A detailed, ship-by-ship review was used to estimate emissions from ships transiting offshore Santa Barbara. The inventory process gathered information on ship names, arrival and departure dates and direction, ship type (e.g., container, bulk carrier), flag, dead-weight tonnage, and average cruise speed. Port Hueneme<sup>15</sup> and the Marine Exchange of Los Angeles - Long Beach Harbor, Inc.<sup>16</sup> were the main sources of these data.

All ships that arrived from the north to Port Hueneme, the Port of Los Angeles or the Port of Long Beach, or departed to the north from any of these ports, were included in the estimates. Duplicates were eliminated. The average cruising horsepower for each ship's main engine(s) was determined using methods detailed in the ARCADIS report, or by consulting the Lloyd's Registry of Ships.<sup>17</sup> Emissions from auxiliary engines were included. We determined the Santa Barbara coastline transit time for each ship, and applied NO<sub>x</sub> emission factors from the ARCADIS report. The factors used were based on ARCADIS' analysis of NO<sub>x</sub> emissions limits finalized in late 1997 at the International Maritime Organization, and considered emissions testing of ships performed as part of Lloyd's Marine Exhaust Emissions Research Programme.<sup>18</sup>

Figure 1 presents a summary of the number of transits along Santa Barbara during 2000 by vessel registry.

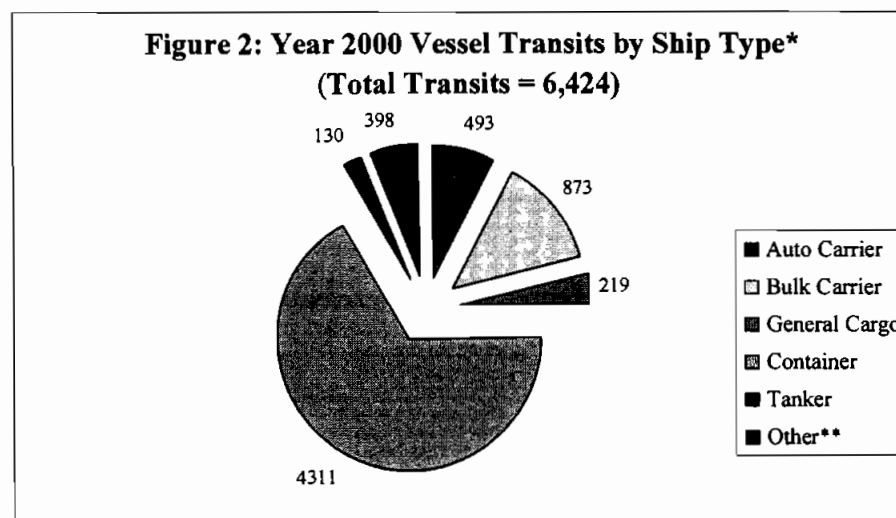


\* 2000 Marine Exchange Data – Ports of Los Angeles/Long Beach.

\*\* Comprised of 37 other countries.

During the year 2000, there were 6,424 vessel transits along Santa Barbara County from 49 different countries. The country with the greatest number of vessel transits was Panama (1,353 transits), followed by the United States (838 transits), and Liberia (721 transits). More than 87 percent of the total transits along this coastline were by foreign-flagged vessels.

Figure 2 itemizes the types of vessels that traversed our coastline during 2000.

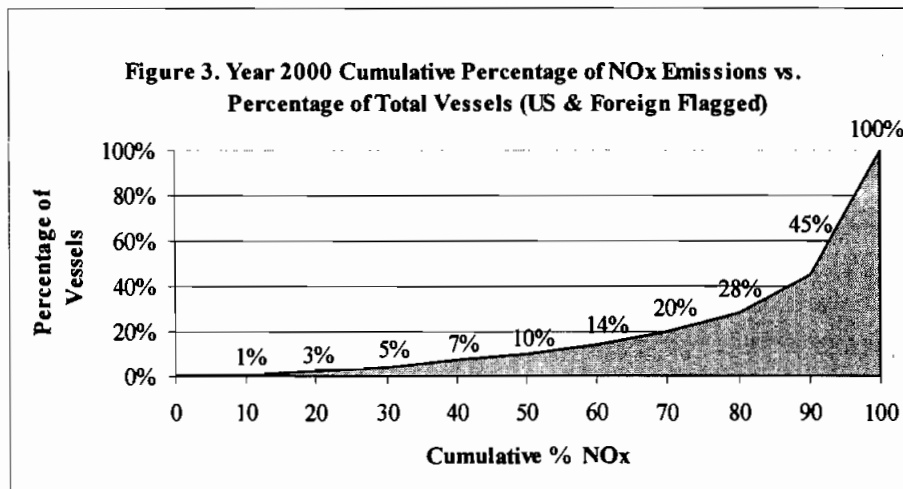


\* 2000 Marine Exchange Data – Ports of Los Angeles/Long Beach.

\*\* Other vessels include Passenger, Reefer, and Ro-Ro vessels.

Figure 2 shows that 67 percent of the 6,424 traverses along our coastline in the year 2000 were by container vessels, followed by bulk carriers (14 percent), auto carriers (8 percent), general cargo vessels (3 percent), and tankers (2 percent).

Figure 3 shows a comparison of the cumulative percentage of NOx emissions versus the percentage of vessels for 2000 offshore Santa Barbara.



Source: 2000 Marine Exchange Data, Ports of Los Angeles/Long Beach

This figure shows that by focusing our retrofit efforts on only 10 percent of the vessels that transit along our coastline, we can target 50 percent of the NOx emissions associated with shipping activities impacting our air quality.

Table 1 presents the maximum and average horsepower ratings by vessel type for those vessels that traversed our coastline during 2001.

**Table 1: Maximum and Average Horsepower Ratings by Vessel Type<sup>19</sup>**

Vessel Type	Maximum Horsepower	Average Horsepower
Auto Carrier	20,940	10,430
Bulk Carrier	20,874	7,742
Container Ship	109,600	32,322
General Cargo	57,089	7,738
Passenger	62,370	30,913
Reefer	15,079	11,267
Ro-Ro	26,921	11,056
Tanker	29,422	8,778

Table 1 shows that the container vessel fleet averaged 32,000 horsepower with a maximum horsepower rating of 109,000. General cargo and passenger vessels had maximum horsepower ratings around 60,000 with the remaining vessels maximum horsepower ratings ranging from 20,000 to 30,000.

The combination of the large number of vessel transits along our 130-mile coastline and the high percentage of container vessels that have the highest average and maximum horsepower ratings (equating to higher emissions) resulted in more than 33 tons per day of NOx emissions in the area in 2000. Foreign-flagged vessels accounted for 87 percent of the total transits, but accounted for 91 percent of the total NOx emissions, since these vessels are predominantly large, higher emission container ships.

## **SHIPPING EMISSIONS IN THE CONTEXT OF SANTA BARBARA COUNTY AIR QUALITY PLANNING**

APCD has prepared several air quality plans for Santa Barbara County to comply with state and federal ozone standards, and offshore emissions have been considered significant in these documents for some time. The first two plans, the 1979 Air Quality Attainment Plan and the 1982 update were prepared in response to mandates established by the federal Clean Air Act Amendments of 1977. The 1982 update predicted attainment of the federal ozone standard by 1984, but acknowledged that the county's ability to attain the federal ozone standard was uncertain because pollution generated offshore was not considered.

In the 1994 Clean Air Plan, photochemical air quality modeling was performed for the region. This modeling showed that emissions from marine shipping activities contributed to ozone formation, and found that Santa Barbara County would attain the federal 1-hour ozone standard by the mandated 1996 attainment date but for the emissions generated off the coast by marine shipping activities.<sup>20</sup>

Santa Barbara County was unable to attain the federal 1-hour ozone standard by the 1996 attainment deadline, and was reclassified in 1997 as a "serious" nonattainment area by the USEPA. The new classification required additional regulatory requirements and the development of another air quality plan to show attainment by a new deadline of November 15, 1999.

Subsequent to the development and submission of the next air quality plan (1998 Clean Air Plan) required to comply with the "serious" nonattainment area mandates, air quality monitoring data showed that the county met the federal 1-hour ozone standard by the 1999 attainment deadline. This prompted the development of a "Maintenance Plan," which became the 2001 Clean Air Plan.

The Maintenance Plan required APCD to determine an "attainment inventory" for Santa Barbara County against which to compare future predicted emissions through 2015. Since the federal 1-hour ozone standard was attained from 1997 through 1999, emission inventories were developed for 1999 for both reactive organic compounds (ROC) and NOx.

The attainment inventory methodology assumes that the emission levels experienced in Santa Barbara County during 1999 are adequate to keep measured ozone concentrations below the federal 1-hour ozone standard. The maintenance demonstration must show that

predicted future year emission levels through 2015 are below the attainment inventory established for 1999.

## **2001 Clean Air Plan Emission Inventory**

This section describes the baseline emission inventory used in the development of the 2001 Clean Air Plan. The emission inventory accounts for the types and amounts of pollutants emitted from a wide variety of sources, including on-road motor vehicles and other mobile sources, fuel combustion at industrial facilities, solvent and surface coating usage, consumer product usage, and emissions from natural sources. Emission inventories are used to describe and compare contributions from air pollution sources, evaluate control measures, schedule rule adoptions, forecast future pollution, and demonstrate attainment and maintenance of air quality standards.

### ***Emission Inventory Development***

The emission inventory is organized in a three-tier hierarchy that categorizes all air pollution sources. The first tier of this hierarchy contains four divisions:

- Stationary sources (e.g., internal combustion engines, boilers, mineral processing)
- Area-Wide sources (e.g., consumer products, paints and solvents)
- Mobile sources (e.g., cars, trucks, planes, trains, ships)
- Natural sources (e.g., vegetation, oil and gas seeps).

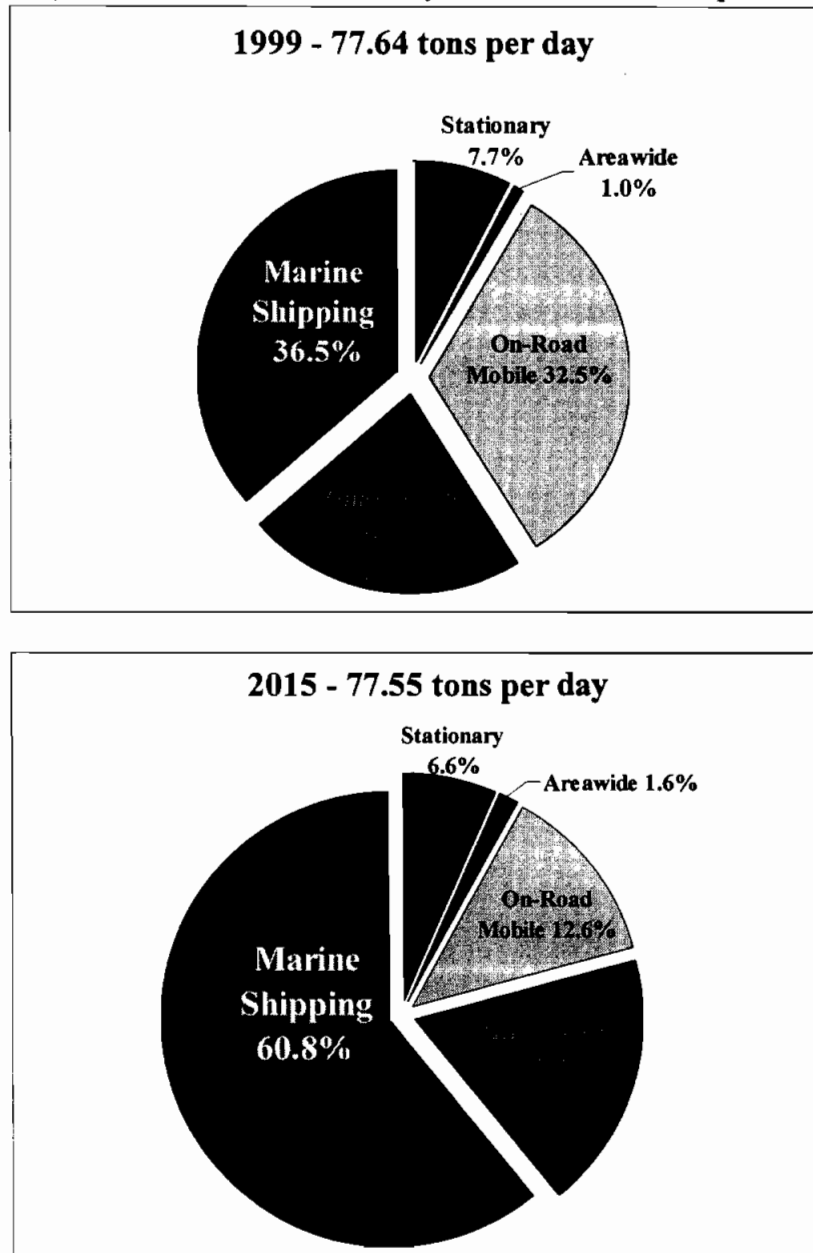
In the second tier, each of the four divisions is sub-divided into major source categories. The third tier divides the major source categories into summary categories. For the purposes of this paper, we present NO<sub>x</sub> emissions by first tier emission divisions for stationary, area-wide, and mobile sources both onshore and offshore of Santa Barbara County, with marine shipping emissions distinguished from the “other mobile” sources. Natural sources are not included in this paper as those emissions are not human-generated.

### ***1999 and 2015 Emission Inventories***

Once the 1999 emission inventory was developed using the most current data, it was forecast out to 2015 using both growth and control assumptions. Growth assumptions include changes in population, employment, vehicle miles traveled, agricultural acres in use, and many others. Control assumptions predict the expected emission controls that will result from local, state and federal air programs. The combination of both growth and control data assumptions are applied to the 1999 inventory in order to develop the 2015 forecast. Figure 4 presents the emission inventories developed for 1999 and forecast for 2015.



**Figure 4: Santa Barbara County NOx Emissions Comparison**

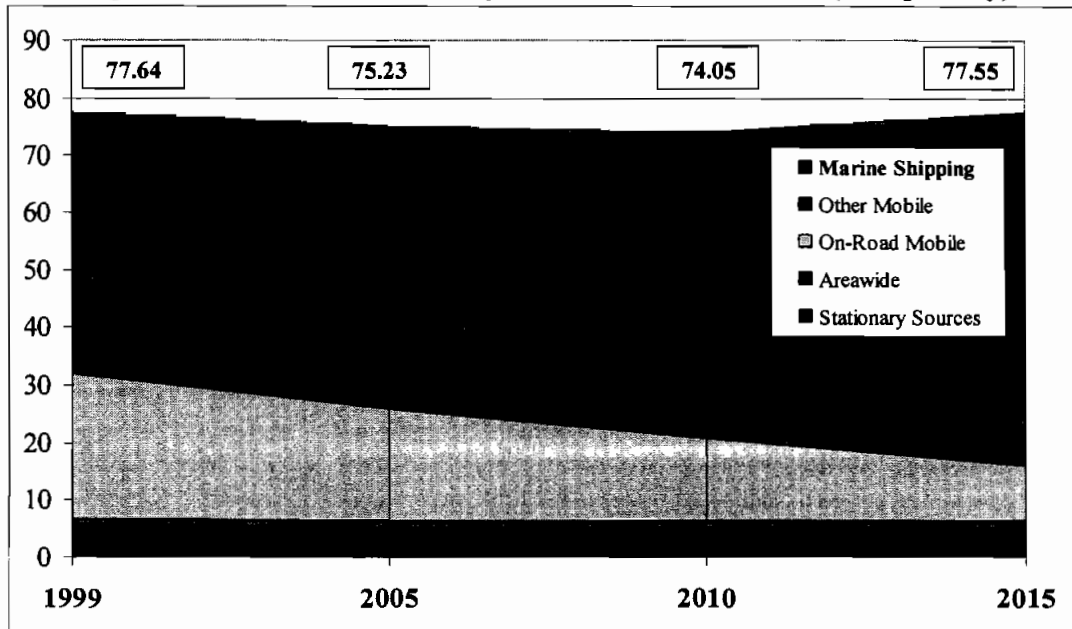


As seen in Figure 4, marine shipping activities contribute more NOx emissions to Santa Barbara County than all the cars, trucks, and buses operating onshore, and represent 36 percent of the total NOx emissions in 1999. The figure also shows that marine shipping emits more NOx than all the “other mobile” sources in the county, including trains, planes, off-road vehicles, farm and construction equipment and many other sources. In addition, Figure 4 shows that the anticipated growth of marine shipping emissions results

in a NOx emission contribution of 60 percent of the total inventory by 2015, almost five times the emissions associated with on-road motor vehicles.

Figure 5 presents the forecast for NOx emissions from 1999 through 2015.

**Figure 5: Santa Barbara County Forecast NOx Emissions (tons per day)**



This figure shows that total NOx emissions decline slightly from 1999 through 2010 and then increase through 2015 to levels that approach those experienced during 1999. This figure also documents that the projected increase in marine shipping emissions essentially negates all the NOx emissions reductions expected to occur onshore from local, state and federal air programs.

## **IMPLICATIONS FOR MEETING AIR QUALITY STANDARDS**

Since forecasted NOx emission levels in 2015 are approaching those experienced in 1999, the county's maintenance demonstration to USEPA comes under increasing scrutiny. If marine shipping emissions continue at the projected rates without any additional controls, Santa Barbara County's long-term trend of improving air quality and ability to maintain attainment of standards could be jeopardized.

Marine shipping activities are the most significant source of emissions that impact our local air quality. And the fact that the growth of marine shipping emissions is counteracting the emission reductions achieved onshore via regulatory controls is of greatest concern. Local, state and federal air programs, in existence for more than 30 years, have resulted in significant emission reductions to date and are anticipated to provide additional emission reductions into the future, as Figure 5 illustrates.

However, the issue at hand is that the majority of the cost-effective emission controls available onshore have been implemented or are already scheduled for implementation. Additional onshore controls will be difficult to obtain and expensive to implement. Reducing emissions from marine shipping activities is of critical importance to the long-term air quality of Santa Barbara County.

## **REGULATORY FRAMEWORK**

Although the shipping industry is highly regulated in some environmental areas such as sewage and waste, and ballast water, regulatory efforts to date to reduce air emissions from marine shipping have not kept pace with emission reduction programs onshore. MARPOL 73/78 is the International Convention for the Prevention of Pollution from Ships. Annex VI, adopted by the Parties to MARPOL in 1997, has NO<sub>x</sub> requirements for the Category 3 engines typically used in ocean-going vessels, beginning January 1, 2000. This Annex has not been ratified by the required minimum of 15 member countries representing 50 percent of the world's merchant shipping.

However, since the NO<sub>x</sub> emission standards contained in Annex VI are retroactive to January 1, 2000 once the Annex is ratified, virtually all ship engine manufacturers already build engines that meet these standards. No additional emission reductions from ratification of Annex VI are expected, although ratification does represent a first step toward the implementation of additional technology-forcing standards and requirements in the future.

The USEPA Final Rule on Control of Air Pollution from New Marine Compression-Ignition Engines at or Above 37 kW (50 hp), effective 1/28/2000, applies to Category 1 and 2 engines, and recommends that the IMO adopt regulations for Category 3 engines that are more stringent than the Annex VI requirements. In 2000, the Bluewater Network settled a lawsuit against the USEPA for failure to establish standards for Category 3 engines. The settlement required USEPA to establish standards for these engines by January 2003. The resultant regulation recently promulgated by USEPA establishes standards that are no more stringent than those established in Annex VI.<sup>21</sup>

CARB is currently developing proposed emission control strategies for commercial marine vessels and ports that are expected to become part of the South Coast Air Quality Management District's State Implementation Plan.<sup>22</sup> These strategies will provide emission reductions statewide. Measures under consideration include:

- setting more stringent emission standards for new harbor craft and ocean-going ships;
- developing ways for existing harbor craft fleet to use cleaner engines and fuels;
- designing strategies to clean up the existing ocean-going fleet; and
- taking steps to reduce land-based emissions at ports.

Action on the state's proposed measures is expected between 2003 and 2005, with implementation in the 2003-2010 timeframe.

Even in the best-case scenario—if new regulations are adopted by CARB and USEPA, and the IMO moves to strengthen standards under Annex VI— it could be many years before significant emission reductions are realized through the regulatory process, particularly for the larger ocean-going vessels that traverse the Santa Barbara coastline. Most of the USEPA and IMO regulations only apply to newly manufactured vessels. Since the turnover of vessels is very slow, coastal and port areas will be living with pollution from existing vessels for many years. Therefore, it is imperative to develop partnerships and incentive programs like those being evaluated by CARB, and to initiate demonstration projects to reduce emissions from the existing vessels that transit our area.

## TECHNOLOGIES

Until recently, many have viewed shipping industry emissions as fairly minor, of lesser impact to onshore air quality, and difficult, if not impossible, to control. Over time, these views have changed in recognition of the facts that a significant percentage of total man-made emissions are from ships, these emissions have both near-shore and regional air quality impacts, and feasible technologies are available at reasonable costs to clean up ship emissions.<sup>23</sup>

Most NOx emissions in exhaust gases are produced due to high temperatures during the combustion process. There are primary methods to reduce NOx formed during combustion, most of which attempt to reduce the maximum temperatures during combustion, as well as secondary methods that treat the post-combustion exhaust gas stream to reduce NOx. Examples of each method are shown below:

### Primary:

- Engine related: injection timing retard, higher compression ratios, increased charge air
- Fuel injection: nozzle changes and injection rate shaping
- Addition of water: fuel-water emulsion, direct water injection, pre-treatment of combustion air (humid air motor or combustion air saturation systems)
- Exhaust gas recirculation

### Secondary:

- Selective catalytic reduction (SCR) mixes exhaust gas with ammonia or urea before it passes through a catalytic bed
- Electrostatic precipitators to reduce PM emissions
- Oxidation catalysts to reduce CO and HC
- Low-sulfur content fuel that allows catalytic converters

In addition to the noted control technologies, operational limits that reduce emissions can also be implemented. The voluntary speed reduction program that limits the speed of ships entering the Ports of Los Angeles and Long Beach is an example of setting operational limits to achieve emission reductions.

Both primary and secondary control technologies are applied most easily to a specific ship during the ship's design stage. Application of these technologies as retrofit controls (i.e., not as part of a ship's original design) has potential downsides, including: high unit cost; ship downtime for installation of the new controls; increased fuel use (typical for timing retard and water injection or emulsion systems); the need for large amounts of deionized water production and storage (typical for water injection, emulsion, and humid air motor systems); potential engine damage from the control system (possible with exhaust gas recirculation that routes exhaust gas particulate matter through the charge air system); and lack of space on the existing ship (e.g., installing SCRs on 2-stroke engines).

In addition, significant modifications to an engine not previously subject to the NOx Technical Code of MARPOL 73/78 of Annex VI may make the engine subject to the Annex VI requirement to demonstrate that the modifications did not cause an increase in emissions. This means that pre- and post-modification emissions tests may be required, even for engines not previously subject to Annex VI requirements.

Table 2 presents a summary of various retrofit control technologies that could be installed on large vessel engines.<sup>24</sup>

**Table 2: Performance Attributes Summary of NOx Control Technologies for Existing Engines.**

Control Technology	Nominal NOx Reduction (%)	Nominal Reduction in PM and other Pollutants (%)	Nominal Increased Fuel Use (%)	Net Present Value (\$)	Global Cost Effectiveness (\$/ton NOx)
Aftercooler upgrade	10	-1	2	\$184,000	\$620
Engine derating	14	-10	4	\$386,000	\$933
Fuel pressure increase	14	-21	2	\$220,000	\$523
Injector upgrade	16	-21	2	\$192,000	\$410
Injection Timing Retard	19	-11	4	\$363,000	\$618
Water in combustion air	28	1	3	\$365,000	\$468
Exhaust gas recirculation	34	-51	0	\$16,900,000	\$16,377
Water/fuel emulsion	42	15	2	\$325,000	\$284
Selective catalytic reduction	81	0	0	\$475,000	\$227

As this table shows, a range of control technologies can be evaluated as retrofits to existing vessels in order to reduce NOx emissions, and these controls potentially carry a lower cost per ton of emission reduction than most typical onshore emission controls. In addition, focusing retrofit efforts on the "frequent flyer" vessels that create the most emissions will provide the most cost-effective emissions reduction projects.

A review of cost-effectiveness calculations for incentive programs,<sup>25</sup> generation of emission reduction credits,<sup>26</sup> and emission control measures<sup>27</sup> shows a range of cost from \$660 to more than \$40,000 per ton of NOx reduced. By way of comparison, the average cost per ton for industrial NOx emission reduction credits used in Santa Barbara County

from 1999 through 2003 was more than \$9,000, and the average cost per ton from California's Carl Moyer Program (Years 1 and 2) was \$5,000.

Comparatively, emission reduction programs for marine shipping applications have the potential to produce significant levels of emission reductions on a more cost-effective basis. This is due to the fact that onshore emission reduction programs have matured, while marine shipping emissions have been largely unregulated to date.

However, the cost-effective emission reductions from marine shipping require a large capital expenditure as indicated by the Net Present Value costs associated with the technologies identified in Table 2 that range from \$184,000 to several million dollars. A broad-based partnership/incentive approach will be necessary to support capital expenditures of this magnitude, and provide for the evaluation, implementation and verification of these technologies through demonstration programs. Once a technology or set of technologies is proven, additional funding partnerships and incentives will be needed to expand implementation programs to other existing vessels.

Table 2 also highlights the potential for increases in other pollutants (e.g., particulate matter, greenhouse gases) and decreased fuel efficiency. These trade-offs need to be clearly identified and minimized to the greatest extent feasible. For example, injection timing retard generally reduces NOx emissions, but increases PM, and increases fuel use with an associated increase in greenhouse gas emissions. A thorough review of each emissions reduction technology must be conducted for each application to avoid emission trade-offs that may be counter to broader clean air goals.

Fuel characteristics can also be modified to reduce pollution, primarily by reducing sulfur content, thereby reducing SOx emissions, and allowing the use of catalytic treatment of exhaust gases to reduce NOx. SOx emissions reduction is a major concern in much of Europe, due to the impacts of acid rain.<sup>28, 29</sup>

There is a tremendous opportunity to reduce both SOx and NOx emissions by reducing the sulfur content of fuels used in shipping. The current average sulfur content of heavy fuel oils used by large marine vessels is about 2.5% (25,000 ppm). The fuel sulfur content limits of the impending IMO Annex VI are set at 4.5% (45,000 ppm), with a 1.5% (15,000 ppm) limit for SOx Emissions Control Areas (SECA) such as the Baltic Sea. Upon application to IMO after Annex VI is implemented, other areas (e.g., coastal areas of the United States) may be declared SECA areas with the 1.5% sulfur limit. These sulfur content values contrast with the current California on-road diesel limit of 0.05% (500 ppm), especially as the sulfur content of typical on-road diesel fuel is usually well below this limit, generally in the 130-150 ppm range. Also, ultra low sulfur diesel (15 ppm sulfur) is now becoming available, and will soon be required on both urban buses and solid waste collection vehicles in California. This ultra low sulfur diesel requirement will also apply nationwide for on-road diesel fuel starting in 2007, so it is clear that there are opportunities to improve the quality of the fuels used by the shipping industry.

The above tables and information document the fact that many opportunities exist to achieve emission reductions from existing marine vessels. Steps towards implementation of a demonstration program targeting reductions from existing vessels could include:

- Identification of funding sources, and securing of funding;
- Design of emissions-testing protocols to validate emission reductions;
- Selection of candidate vessels for demonstration projects;
- Development of criteria for judging the success of a demonstration retrofit program;
- Testing of emission-control technologies in real-world use;
- Evaluation of these technologies for widespread use;
- Formulation of a plan for widespread implementation.

However, as previously outlined, due to the significant capital investment required, the development of creative partnerships and innovative strategies is necessary to build momentum for the implementation of retrofit technologies and cleaner-fuels strategies.

## **PARTNERSHIPS AND INCENTIVES**

The Maritime Air Quality Working Group (MWG), led by CARB, is an industry-wide group of stakeholders including air agencies (CARB, USEPA, and local air districts), environmental groups, and shipping industry representatives (owner operators, ship captains, major engine manufacturers, technology vendors and marine consultants). The group's goal is to gain a basic understanding of the shipping industry, identify control technologies that can reduce NOx and PM emissions from ship engines, and determine how to make these technologies attractive for both retrofit and new implementation by carriers.

The MWG has had several meetings over the last year that have incorporated presentations on available and developing control technologies, and the group is currently reviewing vendor proposals to demonstrate retrofit control technologies on ship engines at sea. The APCD participates in this working group and is interested in seeing cost-effective control technologies successfully installed on one or two ships over the next year.

The US Department of Transportation Maritime Administration (MARAD) is pursuing in parallel a program to review, select, install, demonstrate and test emissions of retrofit control technologies for reducing NOx emissions of large ship engines. MARAD is investigating possible incentive programs to encourage control technology installation on coastal vessels, and will determine if these technologies increase combustion efficiency, thereby saving fuel and reducing greenhouse gases. It is likely that the MARAD demonstration will be the first partnership project for the MWG stakeholders.

Business for Social Responsibility (BSR) is a consortium of businesses interested in improving the environmental and social impact of their operations, and of their suppliers. Among many other programs, BSR has formed a Clean Cargo Program to encourage the

ship owner operators – their “carriers”- to reduce emissions from their sea transport operations.

A range of incentive programs that could be evaluated include:

- Emission reduction credits – A system in which credits are provided for reducing vessel emissions that can be traded within a market-based system.
- Differential port fees – A system where cleaner vessels pay lower fees and dirtier vessels pay higher fees with a net result equal to the existing fee structure.
- Government incentives – Similar to California’s Carl Moyer Program in which funds are allocated to cost-effective projects, based on the merits of the project and the level of cost share funding.
- Environmental award programs – A system in which cleaner vessels are provided the recognition and positive publicity for being the cleanest of the fleet.
- Preferential port access – A system in which the cleanest vessels have the best access to port facilities.

These types of incentive programs need to be carefully evaluated as part of the effort to reduce emissions from the existing fleet. Without some type of incentive program, the information and experience gained in retrofit demonstration projects may not be realized due to the large capital costs associated with many of the technologies discussed in this paper.

It is important to coordinate efforts toward understanding the dynamics of the shipping industry, and researching and demonstrating control technologies by building partnerships, evaluating incentive programs, and sharing results. Only with a cooperative, partnership-based approach will we realize emission reductions from the existing vessels that transit along the Santa Barbara coastline and other areas nationally and globally.

## CONCLUSIONS

As documented in the Santa Barbara County emissions inventories, marine shipping emissions currently impact onshore air quality, and, if left uncontrolled, will be of increasing concern in the future. Conclusion points of interest are listed below.

- Marine shipping emissions are significant and largely unregulated locally, nationally and globally.
- If marine shipping emissions continue to increase without controls, they may threaten attainment strategies of coastal (and inland) areas. This could increase the need to reduce emissions onshore, where many of the most achievable and cost-effective reductions have either already been obtained or are in process.
- International and national regulatory efforts have been largely ineffective to date, and should be strengthened to set targets for development of new engine technologies.
- While regulatory strategies are important to reducing these emissions in the long term, a near-term strategy is needed for existing vessels.



- Many control technologies are available that can potentially reduce emissions in the near term from existing marine vessels at a relatively low cost per ton of NOx reduced. In fact, these technologies are significantly more cost-effective than typical onshore emission controls.
- Retrofit of existing vessels with emission controls will demand a high capital expenditure.
- A coordinated partnership-based approach will be necessary to support the capital expenditure, and provide for the evaluation, implementation and verification of retrofit technologies through demonstration programs.
- Once a technology or set of technologies is proven, additional funding partnerships and incentives programs will be needed to expand implementation programs with existing vessels.

## ACKNOWLEDGMENTS

The Santa Barbara County Air Pollution Control District would like to acknowledge the many individuals and organizations who have assisted us on this project including APL (Capt. Julio Soares), Business for Social Responsibility (Michelle Lapinski), California Air Resources Board (Peggy Taricco, Paul Milkey), Environmental Protection Agency (Jack Broadbent, Roxanne Johnson), Lloyd's Register-Fairplay Ltd. (Richard Veale), Marine Exchange of Los Angeles – Long Beach Harbor, Inc. (Captain Dick McKenna), Maritime Administration (Bob Behr, Danny Gore), Matson Navigation Co. (Kelly Lawson, Ramani Srinivasan), MAN B&W (Kjeld Abbo, Niels Kjemtrup), Port of Hueneme – Oxnard Harbor, and Wärtsilä-Sulzer (Tapio Markkula, Sandra Aufdenblatten, Britt-Mari Kullas-Nyman).

## KEY WORDS

Marine Shipping, Marine Shipping Emissions, Compression Ignition Engines, Air Pollution Control, Santa Barbara County, Annex VI, Emission Control Technologies, Clean Air Plans, Container Ships

## REFERENCES

1. MAN B&W. Propulsion Trends in Container Vessels. Propulsion Trends in Tankers. [www.manbw.com](http://www.manbw.com) (accessed January 2003)
2. International Maritime Organization. Study of Greenhouse Gas Emissions from Ships. MEPC 45(8) (March 2000)
3. Port Import Export Reporting Service. Images: Seaborne Trade by Container Ships. [www.jamri.or.jp/eng/image](http://www.jamri.or.jp/eng/image). (accessed November 2002)
4. Davies, M.E., Plant, G., Cosslett, C., Harrop, O., Petts, J.W. BMT Murray Fenton Edon Liddiard Vince Limited, No. 3623. Study on the economic, legal, environmental and practical implications of a European Union system to reduce ship emissions of SO<sub>2</sub> and NO<sub>x</sub>. Final Report for European Commission Contract B4-3040/98/000839/MAR/B1. (August 2000)

- 
5. Kjemtrup, Niels. MAN B&W. Presentation to Maritime Working Group, in Oakland CA (July 2002)
  6. International Maritime Organization. Study of Greenhouse Gas Emissions from Ships. MEPC 45(8) (2000)
  7. USEPA. Final Regulatory Impact Analysis: Control of Emissions from Marine Diesel Engines; EPA420-R-99-026. (November 1999)
  8. Corbett, J.J. and Fischbeck, P.S. Emissions from Waterborne Commerce in United States Continental and Inland Waters. Environmental Science and Technology, 34, 3254-3260. (2000)
  9. Booz-Allen & Hamilton, Inc. For USEPA. Commercial Marine Vessel Contributions to Emission Inventories – Final Report. (October 1991)
  10. MARAD. Air Quality Management and Marine Vessel Emissions on the West Coast of Canada. Paper presented at “Workshop on Maritime Energy & Clean Emissions” in Washington, D.C. (January 2002)
  11. California Environmental Protection Agency - California Air Resources Board, Draft State and Federal Element of South Coast State Implementation Plan Section II Mobile Sources, Marine and Ports chapter. (December 2002)
  12. Santa Barbara County 2001 Clean Air Plan. (December 2002)
  13. ARCADIS Geraghty & Miller, Inc. Marine Vessel Emissions Inventory, Update to 1996 Report: Marine Vessel Emissions Inventory and Control Strategies – Final Report. Prepared for SCAQMD. (September 1999)
  14. McKenna, Capt. Dick. Marine Exchange of Los Angeles – Long Beach Harbor, Inc. Personal communication. Ship movement data for Port of Los Angeles/Port of Long Beach for 2001. (May 2002)
  15. Wallace, Pete. Director of Operations and Maintenance, Port of Hueneme – Oxnard Harbor. Personal communication. (latest February 2003)
  16. McKenna, Capt. Dick. Marine Exchange of Los Angeles - Long Beach Harbor, Inc.
  17. Lloyd’s Register of Ships on CD-ROM. Version 2.9. (October 2002)
  18. Lloyd’s Register of Shipping, Environmental Engineering Department. Marine Exhaust Emissions Quantification Study – Mediterranean Sea. Final Report 99/EE/7044. (December 1999)
  19. Lloyd’s Register of Ships on CD-ROM. Version 2.9. (October 2002)
  20. Santa Barbara County Air Pollution Control District. 1994 Clean Air Plan (November 1994)
  21. 40 CFR Parts 9 and 94. Control of Emissions From New Marine Compression-Ignition Engines at or Above 30 Liters Per Cylinder; Final Rule. As published in the Federal Register (pages 9746-9789) on Friday February 29, 2003.
  22. California EPA, California Air Resources Board. Draft State and Federal Element of South Coast State Implementation Plan. (January 2003)
  23. Corbett, J.J. MARAD. Presentation to “Workshop on Maritime Energy and Clean Emissions” in Washington, D.C. Establishing the Baseline for Measurements and Technology Evaluations (January 2002)

- 
24. Corbett, J.J. and Fischbeck, P. Table: Technologies for Existing Engines: Performance Attributes Summary of NOx Control Technologies for Existing Engines, MEETS 2000. From J.J. Corbett. Carnegie Mellon. Presentation at ASME 1999 ICE Fall Technical Conference. Emissions From Ships: Current and Emerging Engineering, Science and Policy Issues. (October 1999)
25. California EPA and California Air Resources Board. Carl Moyer Program Status Report (April 2001)
26. Santa Barbara County Air Pollution Control District. Emission Reduction Credit Costs – Santa Barbara County [www.sbcapcd.org/eng/nsr/sb\\_costs.htm](http://www.sbcapcd.org/eng/nsr/sb_costs.htm) (accessed January 2003)
27. South Coast Air Quality Management District. Air Quality Management Plan (November 1996)
28. Linger, R. Shipping Emissions Abatement and Trading. Project Charter (Terms of Reference) DRAFT V1.4. (July 2002). [www.seaat.org](http://www.seaat.org) (accessed January 2003)
29. Agren, Christer. The Swedish NGO Secretariat on Acid Rain. The Harm of Emissions. [www.seaat.org](http://www.seaat.org) (accessed January 2003)

Third  
Edition

Petroleum  
Refineries

Liquid  
Petroleum  
Pipelines

Petroleum  
Products  
Distribution  
and Marketing

Oil and  
Natural Gas  
Production  
Operations

Marine  
Transportation

Cyber/  
Information  
Technology for  
the Petroleum  
Industry

# Security Guidelines for the Petroleum Industry

1100101  
0000100  
010101  
000101  
011110  
1101101  
111010  
00100

American Petroleum Institute  
April 2005

## SPECIAL NOTES

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

API is not undertaking to meet the duties of employers, manufacturers, or suppliers to warn and properly train and equip their employees, and others exposed, concerning health and safety risks and precautions, nor undertaking their obligations under local, state, or federal laws.

Information concerning safety and health risks and proper precautions with respect to particular materials and conditions should be obtained from the employer, the manufacturer or supplier of that material, or the material safety data sheet.

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. Sometimes a one-time extension of up to two years will be added to this review cycle. This publication will no longer be in effect five years after its publication date as an operative API standard or, where an extension has been granted, upon republication. Status of the publication can be ascertained from the API Standards department telephone (202) 682-8000. A catalog of API publications, programs and services is published annually and updated biannually by API, and available through Global Engineering Documents, 15 Inverness Way East, M/S C303B, Englewood, CO 80112-5776.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this standard or comments and questions concerning the procedures under which this standard was developed should be directed in writing to the Director of the Standards department, American Petroleum Institute, 1220 L Street, N.W., Washington, D.C. 20005. Requests for permission to reproduce or translate all or any part of the material published herein should be addressed to the Director, Business Services.

API standards are published to facilitate the broad availability of proven, sound engineering and operating practices. These standards are not intended to obviate the need for applying sound engineering judgment regarding when and where these standards should be utilized. The formulation and publication of API standards is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 1220 L Street, N.W., Washington, D.C. 20005.

*Copyright © 2005 American Petroleum Institute*

## **FOREWORD**

This document is intended to offer security guidance to the petroleum industry. Individual companies have assessed their own security needs and have implemented security measures they consider appropriate. This document is not intended to supplant the measures adopted by individual companies or to offer commentary regarding the effectiveness of individual company efforts. With respect to particular circumstances, local, state and federal laws and regulations should be reviewed.

Information concerning security risks and proper precautions with respect to particular materials and conditions should be obtained from individual companies or the manufacturer or supplier of a particular material.

API is not undertaking to meet the duties of employers, manufacturers, or suppliers to warn and properly train and equip their employees, and others exposed, concerning security risks and precautions, nor undertaking their obligation under local, state or federal laws.

To the extent this document contains company specific information such information is to be considered confidential.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any federal, state, or municipal regulation with which this publication may conflict.

Suggested revisions are invited and should be submitted to API, RASA department, 1220 L Street, NW, Washington, DC 20005.

## TABLE OF CONTENTS

	Page
Executive Summary .....	vii
1.0 Introduction.....	1
1.1 Scope and Objective.....	1
1.2 Organization of the Document.....	1
1.3 Underlying Basis of this Guidance.....	2
1.4 Other Guidelines and Security References .....	2
2.0 Overview of Terrorism and the Petroleum Industry .....	3
2.1 Background on Terrorism and Security .....	3
2.2 Threat to the Petroleum Industry .....	3
3.0 Threat Assessment.....	4
3.1 The Value of Threat Assessment.....	4
3.2 Threat Assessment Process .....	4
3.3 Security Alert Level Systems.....	6
3.3.1 Introduction .....	6
3.3.2 Department of Homeland Security Alert System (HSAS).....	6
3.3.3 U.S. Coast Guard Maritime Security Levels .....	7
3.3.4 International Ship and Port Facility Security (ISPS) Alert Levels .....	8
4.0 The Security Management System Process .....	8
4.1 Initial Screening .....	9
4.2 Data Gathering .....	10
4.3 Initial SVA.....	10
4.4 Example Elements of a Security Plan .....	12
4.4.1 Security Administration & Organization of the Facility .....	13
4.4.2 Personnel Training .....	13
4.4.3 Drills and Exercises.....	14
4.4.4 Record and Documentation .....	14
4.4.5 Response to Change in Alert Level.....	14
4.4.6 Communications .....	15
4.4.7 Security Systems and Equipment Maintenance.....	15
4.4.8 Security Measures for Access Control, Including Designated Public Access Areas.....	15
4.4.9 Protected/Controlled/Restricted Areas .....	16
4.4.10 Security Measures for Monitoring .....	16
4.4.11 Security Incident Procedures .....	16
4.4.12 Audits and Security Plan Amendments .....	16
4.4.13 Security Vulnerability Analysis (SVA) Report .....	16
5.0 Security Vulnerability Assessment (SVA) Concepts .....	17
5.1 Security Vulnerability Assessment Overview.....	17
5.2 Steps in the SVA Process .....	18
5.3 Estimating Risk Using SVA Methods.....	19
5.4 Definition of SVA Terms .....	19
5.4.1 Risk Definition for SVA.....	19
5.4.2 Consequences (C).....	21
5.4.3 Threat (T) .....	22
5.4.4 Vulnerability (V) .....	22
5.4.5 Target Attractiveness ( $A_T$ ).....	22
5.5 Characteristics of a Sound SVA Approach .....	23
5.6 First Step in the SVA Process .....	23

5.7	SVA Strength and Limitations.....	24
5.8	Recommended Times for Conducting and Reviewing the SVA .....	25
5.9	Risk Control and Mitigation .....	25
5.10	Risk Screening .....	26
6.0	Security Conditions and Potential Response Measures.....	27
6.1	Low Condition—Green .....	27
6.2	Guarded Condition—Blue .....	28
6.3	Elevated Condition—Yellow .....	29
6.4	High Condition—Orange .....	29
6.5	Severe Condition—Red .....	30
7.0	Information (Cyber) Security .....	30
7.1	Introduction.....	30
7.2	Specific Security Guidelines.....	31
7.2.1	Security Policies, Standards and Procedures .....	31
7.2.2	Security Awareness and Education.....	32
7.2.3	Accountability and Ownership .....	32
7.2.4	Data/Information Classification.....	33
7.2.5	Security Vulnerability Assessments .....	33
7.2.6	Physical and Environmental Security .....	33
7.2.7	Access Controls and Identity Management .....	33
7.2.8	Network Security .....	34
7.2.9	Systems Development.....	34
7.2.10	Change Control .....	35
7.2.11	Viruses and other Malicious Code .....	35
7.2.12	Intrusion Detection and Incident Management.....	35
7.2.13	Business Continuity, Business Resumption and Disaster Recovery.....	35
7.2.14	Regulatory Compliance .....	36
7.2.15	Audit (Compliance and Assurance).....	36

## Figures

4.1	Security Management System Process.....	9
4.2	Example Elements of a Security Plan.....	13
5.1	Security Events Evaluated during the API SVA Process .....	18
5.2	API/NPRA Security Vulnerability Assessment Methodology.....	19
5.3	Example Risk Matrix.....	20
5.4	SVA Risk Definition .....	20
5.5	SVA Risk Variables .....	21
5.6	Target Attractiveness Factors.....	23
5.7	Times for Conducting and Reviewing the SVA .....	25

## Tables

3.1	Homeland Security Alert System .....	7
4.1	Examples of Petroleum Facility Assets Subject to Potential Security Risk.....	10
4.2	Examples of Security Risks or Threats in the Petroleum Industry.....	11
5.1	Questions to Determine SVA Approach Needed .....	24
Appendix A	Security Regulations Affecting the U.S. Petroleum Industry .....	37
Appendix B	Glossary and Terms .....	41
Appendix C	Communication of Security Intelligence .....	45
Appendix D	References .....	46



## **EXECUTIVE SUMMARY**

Safe and reliable energy is a vital link in the nation's critical infrastructure. Petroleum products play an important role in our national economy, national security and are integral to the American way of life. As such, security has always been and continues to be a priority across the petroleum industry. The American Petroleum Institute is the petroleum industry's primary trade association. API provides a forum for the industry to come together and discuss important issues with Government, develop industry guidelines and share best practices. From developing industry safe operating practices, to assessing vulnerability at facilities, to coordinating emergency response training, API and its members are committed in taking a leadership role to ensure the safety and security of our workers, our surrounding communities and to provide a transparent flow of reliable energy that we have all come to expect in our daily lives.

In order to help petroleum companies evaluate and respond appropriately to their potential and real security threats, the American Petroleum Institute has worked with other industry associations, government and private companies to prepare this security guidance. The risks from terrorist attacks to the U.S. energy supply vary by segment of the petroleum industry, which is broadly defined as petroleum exploration and production, petroleum refining, pipeline transportation (liquids), marine transportation, and petroleum products distribution and marketing. This document provides general security guidance and other reference data on applicable regulatory requirements, which can be tailored to meet the differing security needs of the petroleum industry.

This security guidance is by necessity general in nature. It is intended to provide an overview of security issues in the petroleum industry and provide general guidance on effective policies and practices. Individual companies, working cooperatively with local officials, are best suited for conducting detailed assessments of their own facilities and assets and determining how to protect them. This is because both potential threats and appropriate security measures vary based on size, location, facility type and existing security measures already in place. Due to the sensitive nature of this information, security screenings, site-security plans and vulnerability assessments should be protected under the company's confidentiality program to ensure that detailed information regarding vulnerabilities, threats and countermeasures is available only to those who need such information.

# Security Guidelines for the Petroleum Industry

## 1.0 Introduction

In order to assist petroleum companies evaluate and respond to security threats, the American Petroleum Institute has:

- Assessed the general types of security risks to the public and to petroleum supplies that each sector may face due to terrorism;
- Identified existing standards, recommended practices, guidance and other operational practices, as well as ongoing initiatives that may mitigate these risks;
- Developed guidance on conducting Security Vulnerability Assessments (SVA)<sup>a</sup> in the petroleum and petrochemical industries;
- Developed Recommended Practices for security for offshore oil and gas operations.<sup>b</sup>
- Worked with the Federal Government, other industry associations and petroleum companies to prepare appropriate guidance.

## 1.1 Scope and Objective

The objective of this document is to provide general guidance to owners and operators of U.S. domestic petroleum assets for effectively managing security risks and provide a reference of certain applicable Federal security laws and regulations that may impact petroleum operations.

Domestic petroleum assets are widely distributed, consisting of over 300,000 producing sites, 4,000 offshore platforms, 600 natural gas processing plants, 160,000 miles of liquid pipelines, numerous crude oil and liquefied natural gas (LNG) offloading ports and terminals, 144 refineries, 1,400 finished product terminals, 7,500 bulk stations and 170,000 gasoline retail stations. The vast majority of these assets are small and geographically remote and do not present a significant security risk to the national economy, national security or public safety. However, the petroleum industry supports taking prudent measures to effectively minimize security risks posed by acts of terrorism where warranted.

Certain petroleum facilities are covered by the Maritime Transportation Security Act of 2002 (MTSA), which was signed into law on November 25, 2002. In compliance with MTSA, the U.S. Coast Guard has promulgated federal rules under 33 *CFR* Subchapter H, Parts 101 – 106 that cover port, OCS and vessel security. These regulations require certain vessels and port facilities that could be involved in a transportation security incident prepare a vessel or facility security plan and submit it to the USCG. See Appendix A for a reference table of Federal security regulations that affect the U.S.

## 1.2 Organization of the Document

This document is organized into seven chapters plus three Appendix items for reference. Chapter 1.0 describes the objectives, intended audience, and scope of the guidance and the various references for other security regulations. Chapter 2.0 includes an overview of terrorism and the petroleum industry. Chapter 3.0 describes a process for a threat assessment including the use of security intelligence and threat-based countermeasures systems such as the Department of Homeland Security Alert System (HSAS) and the USCG Maritime Security (MARSEC) levels. Chapter 4.0 describes the elements of a

---

<sup>a</sup> American Petroleum Institute/National Petrochemical and Refiner's Association Guidance "Security Vulnerability Assessment Methodology, October, 2004"

<sup>b</sup> API RP 70 *Security for Offshore Oil and Natural Gas Operations*, First Edition, March 2003 and RP 70I *Security for International Oil and Natural Gas Operations*, First Edition, May 2004.

security plan and provides a plan outline. Chapter 5.0 includes an overview of security vulnerability assessment. Chapter 6.0 includes security conditions and potential response measures. Chapter 7.0 provides an overview of information (cyber) security. The Appendix items provide useful reference information such as a matrix of certain Federal laws and regulations on security and a glossary of terms and references used to develop this document.

### **1.3 Underlying Basis of this Guidance**

Owners and operators in the petroleum industry can enhance the security of their assets and continuity of business operations through the effective management of security risks. By considering site-specific circumstances, security risks can be managed through a risk-based, performance-oriented management systems approach. The foundation of a security management systems approach is to identify and analyze security threats and vulnerabilities, and to evaluate the adequacy of countermeasures provided to mitigate the threats. Security Vulnerability Assessment (SVA) is a management tool that is flexible and adaptable to a wide range of applications and can be used to assist management in identifying and prioritizing security risks and determining the appropriate type and level of protection required at the local asset level.

The need for and type of security enhancements will be determined based on site-specific factors such as the degree of the threat, the degree of vulnerability, the potential consequences of a security event, and the attractiveness of an asset to an adversary. In the case of the terrorist threat, higher-risk sites are those that have critical importance, are attractive targets to the adversary, have a high level of potential consequences, where assets are vulnerable and the threat is great. In these high-risk situations, security enhancements/countermeasures should be considered that reduce one or several of these items to an acceptable level.

Appropriate strategies for managing security risk can vary widely depending on site-specific factors such as the type of facility (fixed or mobile/remote or urban), the operation involved, the type of substances being stored and processed, and the threats facing the facility. As a result, this guidance does not prescribe specific security measures but provides a means of identifying, analyzing, and reducing vulnerabilities based on the unique needs of the location. Each facility should be evaluated individually by management using the best judgment of applicable practices and appropriate security risk management decisions should be made commensurate with the risks. This recognizes that there isn't a uniform approach to security in the petroleum industry, and that resources should be used effectively to reduce high-risk situations on a priority basis. It is recognized that while all security risks cannot be completely eliminated it can be significantly reduced through implementing an effective security risk management program. The security objectives are to employ four basic strategies to manage the risk, including, Deter, Detect, Delay, and Respond.

All owner/operators are encouraged to seek out assistance and coordinate efforts with federal, state, and local law enforcement agencies, and with the local emergency services and Local Emergency Planning Committee as applicable. Owner/Operators can also obtain and share intelligence, coordinate training, and utilize other resources to help deter attacks and to manage emergencies.

### **1.4 Other Guidelines and Security References**

API has developed this guidance for the petroleum industry as a reference to be used with other available sources. This document does not attempt to provide an all-inclusive list of security considerations, but more as a basis for what might be considered when evaluating and implementing security measures. Additionally, it is recognized that certain information included in a security program needs to remain confidential. Petroleum companies should consider a confidentiality

program to understand what information can be shared and what should remain confidential. Other available resources on security include:

- American Petroleum Institute RP 70, *Security for Offshore Oil and Natural Gas Operations*, 1<sup>st</sup> Ed., April 2003.
- American Petroleum Institute RP 70I, *Security for Worldwide Offshore Oil and Natural Gas Operations*, 1st Ed., May 2004.
- American Petroleum Institute Std 1164, *SCADA Security*, 1<sup>st</sup> Ed., September 2004.
- American Petroleum Institute / National Petrochemical and Refiners Association, "Security Vulnerability Assessment Methodology," October 2004.
- American Chemistry Council, "Site Security Guidelines for the U. S. Chemical Industry," 2001.
- American Chemistry Council, "Implementation Resource Guide for Responsible Care Security Code<sup>®</sup> of Management Practices: Value Chain Activities," 2003.
- American Chemistry Council, "Transportation Security Guidelines for the U.S. Chemical Industry," 2001.
- American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS<sup>®</sup>), "Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites," August 2002.<sup>1</sup>
- DOT, Office of Pipeline Safety, "Pipeline Security Information Circular, Information of Concern to Pipeline Security Personnel, *Security Guidance for Natural Gas, and Hazardous Liquid Pipelines and Liquefied Natural Gas Facilities*," September 5, 2002.
- Sandia National Laboratories, "Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF)".
- U.S. Coast Guard NVIC 11-02 (and other NVICs).

In addition to these references, owners and operators should be aware of applicable local and national laws and regulations. See the reference table included in Appendix A for a list of final security regulations impacting the petroleum industry that were enacted prior to the release of this document.

## **2.0 Overview of Terrorism and the Petroleum Industry**

### **2.1 Background on Terrorism and Security**

The FBI defines terrorism as, "the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives." The number of international terrorist incidents has increased in recent years and the potential threat posed by terrorists has increased<sup>2</sup>. All sectors of the U. S. economy are potentially subject to these illicit activities.

### **2.2 Threat to the Petroleum Industry**

Reports from the Department of Homeland Security (DHS), the U. S. Department of State<sup>3</sup>, the Federal Bureau of Investigation (FBI), have indicated that the petroleum industry may be a target of terrorism due to the inherent nature of the products used and its importance on the national infrastructure. Specifically, the petroleum industry may be a target for terrorism due to the following characteristics:

- The physical and chemical properties of the products handled at petroleum sites
- The importance of petroleum to the national economy
- The importance of petroleum to national security
- The symbolism of the industry as a cornerstone of capitalism and western culture.

Fortunately there is little experience with actual terrorism in the U.S. However, this fact poses a challenge for domestic petroleum owners/operators. As a result, government and industry are working together to better protect the national infrastructure and our national security. Facility owners and operators should establish a close relationship with various sources of intelligence, both at the local and national levels. Certain key sources of intelligence include: the local law enforcement, regional FBI offices, emergency response organizations, USCG Office of Intelligence and Investigations and the Energy ISAC. By providing certain basic awareness training, employees and members of the public can act as the watchful eyes and ears for the company by reporting suspicious activity in and around the facility. Lastly, most domestic petroleum companies operate internationally and in remote regions of the world where security has historically been a significant concern. Domestic firms should where possible, tap that experience to help strengthen its domestic security program.

### **3.0 Threat Assessment**

#### **3.1 The Value of Threat Assessment**

Threat assessment is an important part of a security management system. This chapter describes a threat assessment approach as part of a security management system process. In chapter 5.0 the use of threat assessment in the SVA is explained in greater detail.

A threat assessment is used to evaluate the likelihood of an attack against a given asset or group of assets.<sup>4</sup> It is a decision support tool that helps to establish and prioritize security-program requirements, planning and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability, intent, and impact.

Threat assessment is a process that should be systematically performed and kept current to be useful. The determination of these threats posed by different adversaries leads to the recognition of vulnerabilities and to the evaluation of required countermeasures to manage the threats. Without a specific threat in mind, a company cannot effectively develop a cost-effective security management system.

#### **3.2 Threat Assessment Process**

In characterizing the threat to a facility or a particular asset for a facility, a company examines the historical record of security events and adversaries and obtains available general and localized threat information from government organizations and other sources. It then evaluates these threats in terms of company assets that represent more likely, higher payout targets to those adversaries.

Certain threats are assumed continuous, whereas others are assumed to be variable. As such, this guidance follows the Department of Homeland Security's Homeland Security Advisory System (HSAS) for management of varying threat levels to the industry, which is further explained in section 3.4. It should be noted that other agencies and groups (e.g., the USCG MARSEC Levels) have established threat levels other than HSAS. While these systems differ in the number and description of the threat levels, they provide essentially the same information and may be correlated. The threat assessment determines the estimated general threat level, which forms a baseline. Then

intelligence and threat assessment helps to evaluate situations as they develop. Depending on the increased threat level, different security measures above baseline may be necessary.

While threat assessments are key decision support tools, it should be recognized that, even if updated on a regular basis, threat assessments might not adequately capture emerging threats posed by some terrorist groups. Consequently, a threat assessment must be accompanied by a vulnerability assessment to provide better assurance of preparedness.

Intelligence and law enforcement agencies assess the foreign and domestic threats to the United States. The U.S. intelligence community—which includes the Central Intelligence Agency, the Defense Intelligence Agency, and the State Department's Bureau of Intelligence and Research, among others—monitors the foreign-origin terrorist threat to the United States. The Terrorist Threat Integration Center was established to gather and coordinate information and assess the threat posed by domestic sources of terrorism.<sup>5</sup>

Threat information gathered by both the intelligence and law enforcement communities can be used to develop a company-specific threat assessment. However, it should be understood that much of this information is classified and will not be readily accessible without a security clearance. A company should attempt to identify threats in order to decide how to manage risk in a cost-effective manner. Many companies are exposed to a multitude of threats, including terrorism or other forms of threat. A threat assessment can take different forms, but the key components include:

1. the identification of known and potential adversaries, where such information is available and accurate;
2. the recognition and analysis of their intent, motivation, operating history, methods, weapons, strengths, weaknesses, and intelligence capabilities;
3. the assessment of the threat posed by the adversary factors mentioned above against each asset, and the assignment of an overall criticality ranking for each adversary.

Threats need to be considered from both insiders and outsiders, or a combination of those adversaries working in collusion. An external adversary uses unauthorized access to the facility and systems to destroy or steal a target asset. Insiders are defined as those individuals who normally have authorized access to the asset. Insiders pose a particularly difficult threat, due to the possibility for deceit, deception, training, knowledge of the facilities, and unsupervised access to critical information and assets.

The threat categories that should be considered are those that have the intent and capability of causing major catastrophic harm to the facilities and to the public or environment. Four typical threats that may be included in a SVA are the threat posed by international terrorists, domestic terrorists including disgruntled individuals/'lone wolf' sympathizers, disgruntled employees, and extreme activists. Other adversaries may need to be evaluated as appropriate.

All companies are encouraged to discuss threats with local and Federal law enforcement officials, and to maintain networking with fellow national, regional, and local industrial groups to improve the quality of information relied upon. In particular, owner/operators should coordinate with the Joint Terrorism Task Force offices.

The threat assessment is not necessarily based on precise information. In fact, for most facilities, the best available information is vague or nonspecific to the facility. A particularly challenging part of the analysis can be the absence of site-specific information on threats, particularly the recent concern for international terrorism. A suggested approach is to make a threat assumption that international terrorism is possible at every facility that has adequate attractiveness to that threat.

To be effective, threat assessment must be considered a dynamic process, whereby the threats are continuously evaluated for change. During any given SVA exercise, the threat assessment is referred to for guidance on general or specific threats facing the assets. At that time, the company's threat assessment should be referred to and possibly updated given additional information and assessment of vulnerabilities.

### **3.3 Security Alert Level Systems**

#### **3.3.1 Introduction**

Flexibility provides the basis of operational security due to the dynamic threat environment and the need to apply variable security measures are employed accordingly. Alert levels describe a progressive measure of the likelihood of terrorist actions, from normal to imminent risk of attack or action, based on government or company intelligence information. There are three relevant alert level systems that have been developed by the government and international sources to warn of potential acts of terrorism:

1. **Homeland Security Advisory System (HSAS)**—This five-level alert system is based on the National Threat Advisory System developed by the Department of Homeland Security.
2. **Maritime Security Levels (MARSEC)**—This three-level alert system was developed by the U.S. Coast Guard for use by marine vessels, ports and port facilities.
3. **International Ship and Port Facility Security (ISPS) Code**—This three-level alert system is similar to the MARSEC system and applies to foreign flagged vessels and ports.

The purpose of these systems is to provide clear information to both the private and public sectors about the potential for a terrorist action and to help implement appropriate response measures during a threat crisis.

#### **3.3.2 Department of Homeland Security Alert System (HSAS)**

The Homeland Security Advisory System (HSAS) was established on July 27, 2002. This five level color-coded threat advisory system was designed to improve coordination and communication at all levels of Government and with the American public in the fight against terrorism. HSAS provides a framework to assign threat conditions, which can apply nationally, regionally, by sector or to a specific target. The following factors that may be used to assess the threat are:

- Is the threat credible?
- Is the threat corroborated?
- Is the threat specific and/or imminent?
- What are the potential consequences of the threat?

Threat conditions characterize the risk of a terrorist attack. Protective measures are the steps to be taken by a potential target to reduce their vulnerabilities. The HSAS establishes five threat conditions with associated general protective measures. It must be emphasized that specific protective measures should be developed by the facility based on the unique characteristics of that particular facility and from the findings from a site-specific SVA. Section 6 of this publication provides an in-depth discussion of specific protective measures that owners/operators of petroleum facilities should consider when the national alert level changes.

Following is the HSAS five level alert system and their general protective measures.

<b>Table 3.1—Homeland Security Alert System</b>	
○	Assign emergency response personnel and pre-position specially trained teams;
○	Monitor, redirect or constrain transportation systems;
○	Close facilities;
○	Increase or redirect personnel to address critical emergency needs.
○	Coordinate necessary security efforts with armed forces or local law enforcement;
○	Take additional precautions at public events;
○	Prepare to work at an alternate site or with a dispersed workforce;
○	Restrict access to essential personnel only.
<b>Elevated Condition—Yellow:</b> Significant risk of terrorist attacks. In addition to the previous protective measures, the following may be applied:	
○	Increase surveillance of critical locations;
○	Coordinate emergency plans with local jurisdictions;
○	Assess further refinement of protective measures within the context of the current threat information;
○	Implement, as appropriate, contingency and emergency response plans.
○	Check communications with designated emergency response locations;
○	Review and update emergency response procedures;
○	Provide the surrounding community with necessary information.
○	Refine and exercise preplanned protective measures;
○	Ensure personnel receive training on HSAS, corporate and facility specific protective measures;
○	Regularly assess facility vulnerability and take measures to reduce them.

The National Infrastructure Protection Center, U.S. Coast Guard and other agencies publish guidance on protective measures that are recommended for the different threat levels<sup>6</sup>.

### 3.3.3 U. S. Coast Guard Maritime Security Levels

The U.S. Coast Guard has developed a three-level Maritime Security (MARSEC) alert system for use by marine vessels, certain energy facilities and ports. The MARSEC alert levels are:

- **MARSEC I:** Low or Moderate Threat—this alert is defined as the “new normalcy”.
- **MARSEC II:** Heightened Alert—this alert is used when there is credible intelligence suggesting a high threat, but no specific target or delivery method is known.



- **MARSEC III: Maximum Alert**—this alert is issued when there is credible intelligence coupled with a specific threat.

The U.S. Coast Guard will communicate heightened levels of alert using Maritime Security levels (MARSEC) 1, 2, and 3 that essentially align with the graduated color-coded threat condition levels defined by the Homeland Security Advisory System (HSAS). MARSEC is the maritime sector's tool for communicating risk and is linked to the HSAS.

MARSEC Level 1 generally correspond to the lowest three levels of HSAS: Green (Low), Blue (Guarded), and Yellow (Elevated). MARSEC Level 2 corresponds to HSAS Orange (High), and MARSEC Level 3 corresponds to HSAS Red (Incident Imminent).

Facilities should develop and implement protective measures, to be reflected in their security plans, if necessary, which increase as the MARSEC level increases to reduce the risk of a transportation security incident. MARSEC levels may be assigned for the entire nation, or they may be set for a particular geographic area, industrial sector, or operational activity. It should be noted that it is possible to shift from MARSEC 1 directly to MARSEC 3 without an intermediate shift to MARSEC 2.<sup>7</sup>

Section 6.0 provides in-depth discussion of specific protective measures that owners/operators of petroleum assets may consider when the national alert level changes.

#### **3.3.4 International Ship and Port Facility Security (ISPS) Alert Levels**

The ISPS code is a three-level alert system similar to the MARSEC system.

**Security level 1: (Normal)** The level at which the ship or port facility normally operates. Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

**Security level 2: (Heightened)** The level applying for as long as there is a heightened risk of a security incident. Security level 2 means the level where appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

**Security level 3: (Exceptional)** The level applying for the period of time when there is the probable or imminent risk of a security incident. Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

Setting security level 3 should be an exceptional measure, used only when credible intelligence indicates that a security incident is probable or imminent. Security level 3 should only be set for the duration of the identified security threat or actual security incident. While the security levels may change from level 1, through level 2 to level 3, it is possible that the security levels will change directly from security level 1 to security level 3.

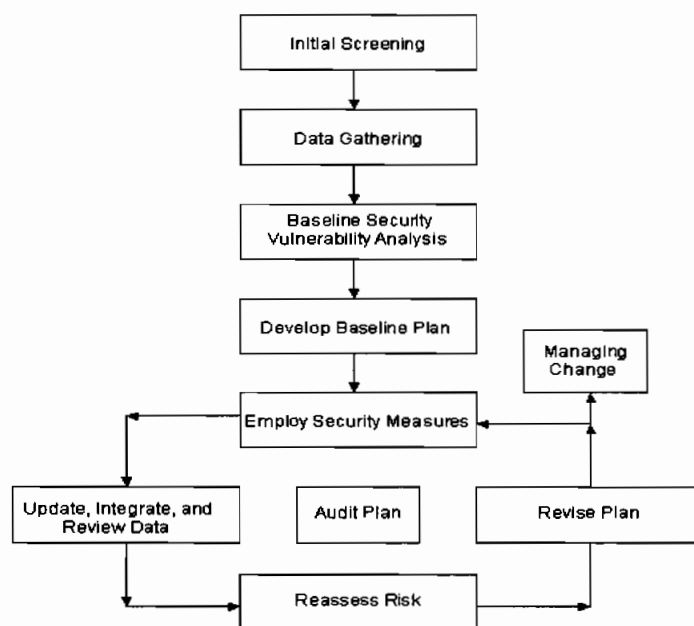
### **4.0 The Security Management System Process**

There is a significant variation in the detail and complexity associated with different SVA methods. Many companies without a formal SVA processes may find that an initial screening level SVA can be beneficial in terms of focusing resources on the most important areas. Companies may find that a screening approach is the most practical means to prioritize facilities for SVA. Depending on the nature of the location and its operations, not all facilities may require a formalized SVA and security plan.

Each owner/office should establish a security management system to effectively manage security risks as appropriate. Since all petroleum operations have unique characteristics, the management system should provide for flexibility and continuous improvement due to changing conditions. However, an effective security management system should have a solid base of several essential elements.

Figure 4.1 illustrates an example of a security management system. The decision flow provides a common process to develop and maintain a site-specific security plan. Owner/operators should consider their unique security risks and then assess those risks to ensure that the plan effectively addresses the highest risks first. There are many different approaches to implementing the elements identified in Figure 4.1, ranging along a continuum from simple to complex. There is no “best” approach that is applicable to all petroleum operations for all situations. This guideline recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

**Figure 4.1—Security Management System Process**



#### **4.1 Initial Screening**

An initial evaluation should be conducted prior to launching a formal SVA. The screen should evaluate petroleum facilities at a “systems level” (high level) by considering the potential economic ramifications, public safety and health impacts, national security and the effects on the value chain (interdependencies) as a result of a significant event. If done at a corporate level, screening can be used to help prioritize which facilities would be candidates for further analysis. Screening can also be helpful when evaluating regional impacts. For those facilities that are identified for further evaluation, a formal SVA should be considered that looks at individual assets within the facility and helps to identify and prioritize vulnerabilities that should be addressed.

## 4.2 Data Gathering

After the initial screening, the first step in an SVA is to assemble information about the location, its assets and any potential threats to those assets. In this element, one performs the initial collection, review, and integration of data that is needed to understand location-specific risks to security. The types of data to support a SVA may include information on the operation, surveillance practices, security measures, and the specific security issues and concerns that are unique. For those that are just formalizing an approach to a security plan, the initial data gathering may be focused on a limited number of assets so that a screening for the most significant security risks can be readily identified.

<b>Table 4.1—Examples of petroleum facility assets subject to potential security risk</b>
<b>Buildings:</b>
Administration offices, corporate offices, control rooms
<b>Equipment:</b>
Process units and associated control systems; product storage tanks; surge vessels, boilers, turbines, process heaters, sewer systems
<b>Support systems:</b>
Utilities such as natural gas lines, electrical power grid and facilities (including back-up power systems), water-supply systems, wastewater treatment facilities
<b>Transportation interface:</b>
Railroad lines and railcars, product loading racks and vehicles, pipelines entering and leaving facility, marine vessels and dock area, off site storage areas
<b>Cyber systems and information technology:</b>
Computer systems, networks, all devices with remote maintenance ports, SCADA systems, laptops, PDAs and cell phones.

## 4.3 Initial SVA

In this element, the data assembled from the previous step is used to conduct a SVA. The SVA begins with a systematic and comprehensive search to identify possible security risks to the facility. Through the integrated evaluation of the information and data collected in the previous step, the SVA process identifies the location-specific security-related events or conditions, or combinations of events and conditions that could lead to loss of security, and provides an understanding of the likelihood and consequences of these events.

There is a significant variation in the detail and complexity associated with different SVA methods. Some companies without a formal SVA processes may find that an initial screening level SVA can be beneficial in terms of focusing resources on the most important areas. Companies may find a screening approach as the most practical means to prioritize facilities for SVA.

**Table 4.2—Examples of security risks or threats in the petroleum industry**

<ul style="list-style-type: none"> <li>• Intentional release (loss of containment) from a process unit or storage tank</li> <li>• Loss of a critical management team or member</li> <li>• Destruction or disruption of support systems, such as: <ul style="list-style-type: none"> <li>○ Electrical power; water supply, sewer systems</li> <li>○ Communications systems, computer systems</li> <li>○ Raw material (crude oil) supply, finished product distribution</li> </ul> </li> <li>• Contamination of raw material or finished product</li> <li>• Bomb threat or discovery of an Improvised Explosive Device (IEDs) or Vehicle Borne Explosive Devices (VBED)</li> <li>• Bio-terrorism or eco-terrorism</li> <li>• Cyber attack</li> <li>• Vandalism or theft</li> </ul>
--

After identifying the most significant risks next determine what countermeasures should be implemented to reduce or eliminate the risk, and where additional assessment techniques would be of the most value in identifying future risk-threatening issues. The risk control and mitigation process may involve:

- Identification of risk control options that lower the likelihood of an incident, reduce the consequences, or both;
- A systematic evaluation and comparison of those options;
- Selection and implementation of a strategy for risk control.

A SVA may also help to identify and prioritize likely targets and avoid expending resources where the likelihood of attack is remote or where the consequence is less than other targets. A tiered, risk-based approach may be the most effective way to evaluate, identify, and prioritize potential targets. There are, however, a number of methods that can be employed to conduct a SVA and identify risk control activities.

**Develop Baseline Security Plan.** Using the output of the SVA, a plan is developed to address the most significant risks and assess the security of the facility or asset. This plan should include the mitigation risk control actions, as well as security assessment activities (e.g., inspections and traffic and personnel control).

**Employ Security Measures.** In this element, the baseline security plan activities are implemented, the results are evaluated, and the necessary changes are made to ensure risks that might lead to system failures are controlled. As noted previously, a SVA may identify other risks that should be addressed.

Examples of physical security elements may include, but are not limited to:

- Controlling access into, within and out of a facility or critical asset areas;
- Perimeter protection including immediately beyond the perimeter;
- Security personnel;
- Redundant systems (electrical, water, computing, communications, sewer, gas);
- Mail and package screening system.

**Update, Integrate, and Review Data.** After the initial security assessments have been performed, the facility will have improved and updated information about the security of the facility. This

information should be retained and added to the database of information used to support future SVAs and security evaluations.

**Reassess Risk.** SVAs should be performed periodically to factor in recent operating data, consider changes to the facility design, and to analyze the impact of any external changes that may have occurred since the last SVA, e.g., adjacent facilities and changes in traffic flow. The results of security assessments, such as inspections and drills, should also be factored into future SVAs to ensure the process reflects the latest understanding of the security issues.

**Revise Plan.** The baseline security management plan should be transformed into an on-going security assessment plan that is periodically updated to reflect new information and the current understanding of security risks. As new risks or new manifestations of previously known risks are identified, additional mitigation actions to address these risks should be performed, as appropriate. Furthermore, the updated SVA results should also be used to support scheduling of future security assessments.

**Audit Plan.** Companies should collect information and periodically evaluate the success of their security assessment techniques and other mitigation risk control activities.

**Managing Change.** A systematic process should be used to ensure that changes to a facility or its operations are evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the facility operates are evaluated. After these changes have been made, they should be incorporated, as appropriate; into future SVAs to be sure the SVA process addresses the facility as it is currently configured. As this final element indicates, managing security is not a one-time process. As implied by the loop in the lower portion of Figure 4.1, a security management system involves a continuous cycle of monitoring conditions, identifying and assessing risks, and taking action to minimize the most significant risks. SVAs should be reviewed and revised to reflect current conditions.

It is important to emphasize that a security plan should be a highly integrated and iterative process. Although the elements depicted in Figure 4.1 are shown sequentially for ease in illustration, there is a significant amount of information flow and interaction between the different steps. For example, the selection of a SVA approach depends in part on what risk related data and information are available. Conversely and while performing a SVA, additional data needs are usually identified to better address potential vulnerability issues.

#### **4.4 Example Elements of a Security Plan**

Security plans should address a number of key elements related to an organization's security policies, practices, and procedures as well as describe the physical and cyber security features being employed to protect a particular asset. Figure 4.2 is an example of certain key elements that may be considered as part of a security plan. Figure 4.2 was created to be consistent with the Maritime Transportation Security Act (MTSA) as required under the U.S. Coast Guard regulations, 33 *CFR* 105.405. If you are a MTSA covered facility, your FSP requirements may be significantly more stringent than those outlined in this document in Figure 4.2. You are therefore encouraged to review USCG Regulations 33 *CFR* Parts 101-106 for more detailed information about your obligations. For a more comprehensive reference of federal laws and security regulations, please refer to Appendix A.

**Figure 4.2—Example Elements of a Security Plan**

1.	Security Administration & Organization
2.	Personnel Training
3.	Drills and Exercises
4.	Records and Documentation
5.	Response to Change in Alert Level
6.	Communications
7.	Security Systems & Equipment Maintenance
8.	Security Measures for Access Control, Including Designated Public Access Areas
9.	Security Measures for Protected/ Controlled/Restricted Areas
10.	Security Measures for Monitoring
11.	Security Incident Procedures
12.	Audits & Security Plan Amendments
13.	Security Vulnerability Analysis (SVA) Report

In general, the security plan should be customized to support each owner/operator's unique needs therefore, not all of the items listed in Figure 4.2 may be necessary at a particular location. It is up to the company determine its security needs based on a sound risk-based decision making process. For more information about security risk-based decision-making, please refer to section 5.0.

The security plan should be periodically evaluated and updated to account for changes in operation, the environment in which the system operates, new data and other security-related information. Periodic plan review and improvement is helpful to take advantage of new information, improved technology, and changes in the operating plan of a facility. For example, the availability of new threat information may require a change in strategy for access control. An effective security plan should be flexible to account for changes in the operating environment and to meet the goals of an organization's management system.

#### **4.4.1 Security Administration and Organization of the Facility**

This section of the security plan should identify the Security Officer and/or the person(s) primarily responsible for administering the security program at the location. Other site/company personnel with security responsibilities should also be identified, along with a description of their duties and responsibilities (e.g., a guard force supervisor, other guards, receptionists that confirm the identification of visitors, etc.).

#### **4.4.2 Personnel Training**

This section of the security plan should describe the security-related training provided to the Security Officer(s) and/or the person(s) primarily responsible for administering the security program at the location. Training for other site/company personnel with security responsibilities should also be identified as well as other security awareness training provided to employees at the location.

For efficiency purposes it is noted that many EHS-training topics, have a direct or peripheral relationship to security (e.g., emergency response, particularly in a petroleum handling/processing facility). These topics should also be described as appropriate. For MTSA facilities, the USCG Regulations under 33 *CFR* 105.205 provide a list of qualifications for Facility Security Officers (FSOs), other persons with security duties, and all other employees respectively. Note that these comprehensive lists of skills do not all have to be explicit training topics. They can be obtained

through either training and/or experience. The training for all other employees of the site is orientation and security awareness, stressing the notion that all employees need to develop a healthy level of skepticism about what they see and hear on or adjacent to the site while performing their normal duties.

#### **4.4.3 Drills and Exercises**

This section of the security plan should describe the planned activities that rehearse aspects of the security plan and any procedures that support the plan. Each location should determine the extent and frequency required to conduct security drills and exercises. Based on a security risk assessment, a specific location may find that no drills or exercises are warranted, others may find that short, focused activities that test one portion of the security program and involve one person or group and their duties (e.g., vehicle searches by main gate guards) will be sufficient, while higher risk sites may require full-scale roll-out or table-top exercises involving multiple groups and offsite responders.

Many of these activities may share the same goals, the same onsite personnel and the same offsite responders as those required for environmental, health, or safety (EHS) related events. Again, efficiency should be considered to minimize any duplication and to leverage existing programs and activities.

For MTSA facilities, the USCG regulations require certain drills and exercises at defined maximum intervals. Many EHS laws and regulations have similar requirements. For example, a petroleum processing facility may be covered by the Oil Pollution Act, SARA Title III regulations, and possibly OSHA and EPA requirements. It is suggested that the EHS and security staffs at the site and corporate levels reconcile these requirements and devise a drill and exercise plan that meets all regulatory requirements simultaneously, including documentation. This plan should then be incorporated into or referenced by the security plan. The security plan should describe, in general terms, the follow-up process for drill and exercise critique action items. If this is the same process that used to resolve EHS-related recommendations and action items, this information can be referenced to the appropriate procedures, databases, or other documents.

In addition to facility drills and exercises, the company's crisis management plan (CMP), if applicable, should also be described in this section of the security plan, to the extent that the security program of the site will rely on the CMP as part of its security program, and what information and support the CMP describes will be provided by the individual site(s). The site emergency response plan(s) and the company CMP are also described and referenced in the security incident procedures section of the security plan.

#### **4.4.4 Records and Documentation**

This section of the security plan should describe what security-related records will be kept and how they will be protected from unauthorized disclosure. To the extent possible, existing EHS, quality, and other recordkeeping systems should be utilized to avoid duplication and overlap. Many petroleum facilities have thorough recordkeeping systems already in place for EHS and/or ISO purposes. Therefore, this section of the security plan should describe how the existing documentation systems will be modified to include security-related matters, and who has the responsibility for maintaining the security records, as well as record retention policies for security-related records. MTSA facilities have eight (8) specific types of records that must be kept.

#### **4.4.5 Response to Change in Alert Level**

This section of the security plan should describe the security alert system in use at the site or company, whether it is the Department of Homeland Security (DHS) Homeland Security Advisory

System color-coded system, U.S. Coast Guard Maritime Security (MARSEC) levels, International Ship & Port Security (ISPS) Code Security Levels, or a company-specific system. Specifically, the security plan should describe what the site would do at each level in the alert system. For example, if the site uses the DHS HSAS alerts, the plan should describe what additional security measures will be employed if the alert level is elevated from Yellow to Orange. Since most of the alert systems are maintained by external government organizations, the security plan should also describe how changes in alert levels are recorded and the time taken to achieve the declared level. Even in the absence of direct regulatory requirements (e.g., the MTSA 12 hour limit to achieve declared level), the site or company might be asked to report this time interval to external organizations. Refer to section 3.4 of this guidance for a more thorough discussion of alert levels. Refer to section 6.0 for certain example response measure related to changes in the alert level.

#### **4.4.6 Communications**

This section of the security plan should describe the necessary communications capabilities of the facility with respect to implementing the security plan. Certain elements to consider are:

- Communications capabilities between employees (e.g., radio, telephone, etc.).
- Communications between the facility and offsite responders or support (e.g., 911).
- Communications between vessels and the facility, if applicable.
- Communication of data, including which computer systems and networks are critical to security (e.g., process control systems; electronic access control systems, etc.), including a general description of the cyber security provisions for these systems.

It should be noted that not all of these elements might be appropriate for a specific location. For example, a small low-risk, unmanned, remote facility may require periodic checks on a weekly or monthly basis.

#### **4.4.7 Security Systems and Equipment Maintenance**

This section of the security plan should describe the inspection, test, and preventive maintenance program for security equipment (e.g., camera systems, lighting fencing, etc.).

#### **4.4.8 Security Measures for Access Control, Including Designated Public Access Areas**

This section of the security plan should include the policies, practices, and procedures that are important to effectively implement the security plan. The following is a list of items to consider. It should be cautioned that not all of these elements may be appropriate for a specific location.

- Identification requirements for employees, visitors, contractors, truck drivers, railroad crews, government employees/law enforcement and other who may seek access.
- Sign-in or documentation of access procedures.
- Escorting policies for visitors, contractors, and government employees. (Circumstances when escorts are required and the procedures to be followed under each situation.)
- Screening and searching procedures for vehicles, baggage (accompanied and unaccompanied), hard-carried articles.
- Physical security measures applicable to access control (Fencing/barriers, locks, lighting, intrusion detection, etc.).
- Physical barriers that prevent vehicles from being used as weapons.
- The escalation in the implementation of access control procedures as alert levels escalate (How vehicle search procedures change as alert levels rise).



#### **4.4.9 Protected/Controlled/Restricted Areas**

If the location designates certain areas as protected, controlled or restricted, then the physical security measures pertinent to those areas should be described this section of the plan.

#### **4.4.10 Security Measures for Monitoring**

This section of the plan should describe how the facility is monitored for unauthorized access. Monitoring can be done through a variety of methods to meet the needs of a particular location. For remote facilities that are considered less attractive, frequency of operational checks may be sufficient. For more sophisticated facilities, a combination of personnel monitoring (guards and dogs) and technology (intrusion detection) may be more appropriate. As with access control measures, the security plan should describe how the monitoring equipment, personnel, and procedures change as alert levels escalate. For example, if the facility employs off-duty law enforcement officers at “Orange” alert, then this arrangement should be described in the security plan.

#### **4.4.11 Security Incident Procedures**

This section of the plan should define what events constitute a breach of security, who is to be notified and the order of such notification. Additionally, the plan should describe the procedure to conduct an investigation of security breaches and incidents (note that this procedure may require some modification to include security related incidents within its scope and to define unique requirements for such investigations). This section should also generally describe or reference the site emergency response plan and the company crisis management plan, if applicable.

#### **4.4.12 Audits and Security Plan Amendments**

This section of the security plan should describe how the plan should be audited, including periodicity, audit team leadership/membership, documentation, and follow-up of findings. For MTSA facilities, the USCG regulations contain specific provisions for security plan audits. Non-MTSA facilities may wish to develop their own or use existing HES auditing.

Following an audit, or for other reasons, the security plan may require amending. The process for generating security plan amendments, how they are approved (both internally, and possibly by external organizations) should be described. The USCG regulations contain a defined interface process between the Coast Guard and the facility to amend a security plan. If the facility is not USCG regulated and is ISO-9000 certified, the ISO process for maintaining controlled documents, or an equivalent may be used.

#### **4.4.13 Security Vulnerability Analysis (SVA) Report**

This section of the plan may include the SVA report as an attachment, a summary of the SVA, or reference the SVA report. The SVA contains the basis for many of the other items described in the security plan and hence becomes a part of the plan. This includes the need to keep the SVA current, as well as the security plan itself. If the facility is Coast Guard regulated, the SVA is referred to as a Facility Security Assessment (FSA) and accomplishes the same purpose as a SVA. Additionally, if the facility is Coast Guard-regulated, the completed Facility Vulnerability and Security Measures Summary (Form CG-6025) must also be included in the security plan. (Refer to Chapter 5.0 for more information on security vulnerability assessment.)

## 5.0 Security Vulnerability Assessment (SVA) Concepts

### 5.1 Security Vulnerability Assessment Overview

Security Vulnerability Assessment (SVA) is a systematic process that evaluates the likelihood that a threat against a facility or asset will be successful and considers the potential severity of consequences to the facility itself, to the surrounding community and on the energy supply chain. One purpose of an SVA is to identify countermeasures that may reduce the risk of an attack and its potential consequences.

There are several SVA techniques and methods available, all of which share common elements. Ultimately, it is the responsibility of the owner/operator to choose the SVA method and depth of analysis that best meets the facility's needs. Differences in geographic location, type of operations, and on-site quantities of hazardous substances, if any, all play a role in determining the level of SVA and the approach taken. Examples include:

1. ***Characterize the facility*** to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure, and the consequences if they are damaged or stolen.
2. ***Identify and characterize threats*** against those assets and evaluate the assets in terms of attractiveness of the targets.
3. ***Identify potential security vulnerabilities*** that threaten the system's service or integrity.
4. ***Determine the risk*** represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur.
5. ***Rank the risk*** of the event occurring and, if high risk, make recommendations for lowering the risk.
6. ***Identify and evaluate risk mitigation options*** and re-assess risk.

The objective of conducting an SVA is to identify security hazards, threats, vulnerabilities and countermeasures that will provide for the protection of the public, workers, national interests, the environment, and the company.

Owner/operators may use any appropriate security vulnerability assessment methodology that effectively achieves this objective. Following are a few published methodologies that are currently available for this use:

- API RP 70 *Security for Offshore Oil & Natural Gas Operations*, 1<sup>st</sup> Ed., March, 2003
- API RP 70I *Security for International Oil and Natural Gas Operations*, 1<sup>st</sup> Ed., April 2004
- API/NPRA *Security Vulnerability Assessment Methodology*, September 2004
- American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS®) "Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites, August 2002"<sup>8</sup>
- Sandia National Laboratories Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF)
- USCG NVIC 11-02

This guidance should also be considered in light of any applicable governmental security regulations and other guidance as outlined in Appendix A, Regulatory Matrix.

The SVA process may be used to assess a wide range of security issues such as those listed in Figure 5.1.

**Figure 5.1—Security Events Evaluated During the API SVA Process**

1. *Loss of containment* of toxic substances or flammable hydrocarbons at the facility from intentional damage of equipment or the malicious release of these materials, which may cause multiple casualties, severe damage, and public or environmental impact.
2. *Theft* of toxic substance or flammable hydrocarbons with the intent to cause severe harm at the facility or offsite.
3. *Contamination* or spoilage of products to cause workers or public harm on or offsite.
4. *Degradation* of assets or infrastructure or the business function or value of the facility or the entire company through destructive malevolent acts.

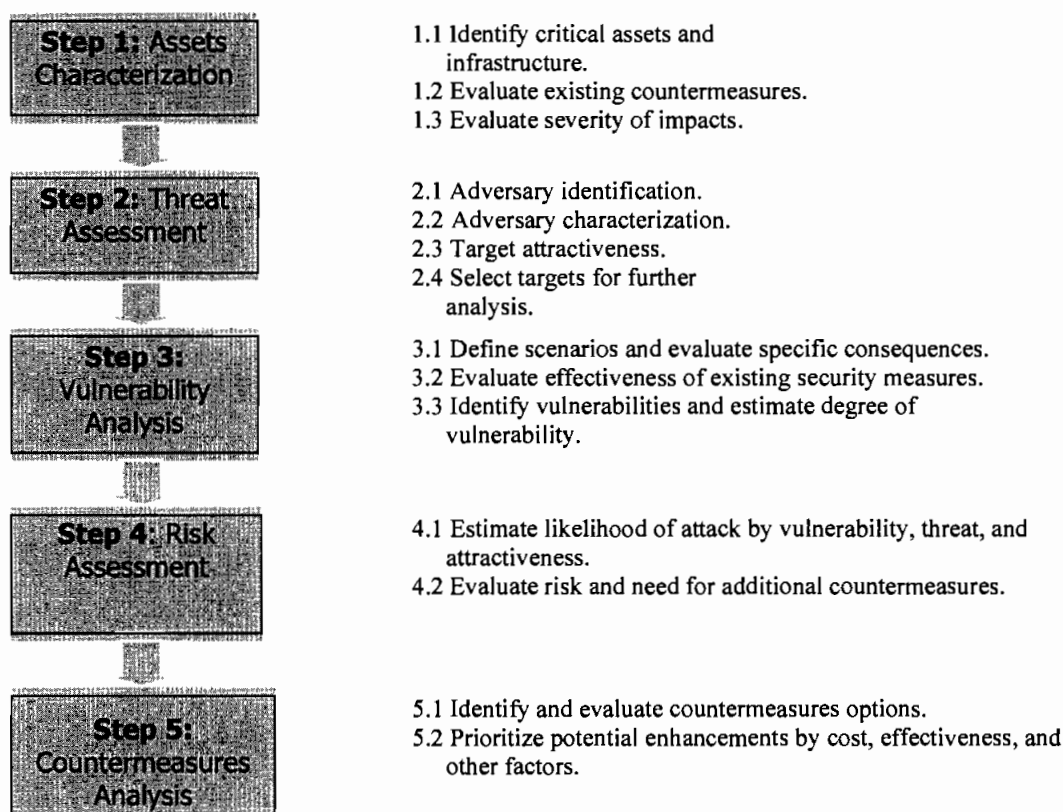
If a facility is covered under USCG regulations 33 *CFR* 101 through 106, there are specific security events that need to be evaluated as part of the SVA. Please refer to the applicable parts of the regulation and U.S. Coast Guard NVIC 11-02 for details on these events, as they are specific to the type of vessel/facility/operation.

## 5.2 Steps In the SVA Process

Figure 5.2 presents the SVA process flow diagram from the API/NPRA Security Vulnerability Assessment Methodology. It should be noted that this approach to conducting security vulnerability assessments has been developed specifically for the petroleum and petrochemical industries. Other valid approaches, such as outlined in API RP 70 and RP 70I, have been developed and are being used successfully within the petroleum industry as mentioned in Section 5.1 above. To obtain a copy of the “API/NPRA SVA Methodology” contact:

American Petroleum Institute  
1220 L. Street, N.W.  
Washington, DC 20005  
(202) 682-8000  
[www.api.org](http://www.api.org)

National Petrochemical and Refiners Association  
1899 L. Street, N.W.  
Washington, D.C. 20036  
(202) 457-0480  
Attn: Maurice McBride

**Figure 5.2—API/NPRA Security Vulnerability Assessment Methodology**

### 5.3 Estimating Risk Using SVA Methods

Risk management principles recognize that risk generally cannot be eliminated, however by enhancing protection from known or potential threats it can be reduced. It is important to make risk decisions about these threats using a systematic method. SVA methods are tools that provide management with risk information based on a thorough, defensible process. However, the quality of the study is dependent on the quality of the inputs and the soundness of the logical relationships inherent in the SVA method used to evaluate the input and output conditions. Much of the threat information that the Government possesses is classified and is not generally available to the public.

### 5.4 Definition of SVA Terms

#### 5.4.1 Risk Definition for SVA

Security risks are different from safety risks. The concept of threat needs to be understood as a combination of an adversary's capability plus their intent. One without the other, and there is no threat.

The petroleum industry has a great deal of experience in managing risks in the safety arena. In that context, risk is usually expressed as a product of probability and consequences. Traditional risk management has focused on the likelihood of an accidental event. In the security realm, this traditional model begins to break down. In the absence of specific intelligence, it is impossible to be

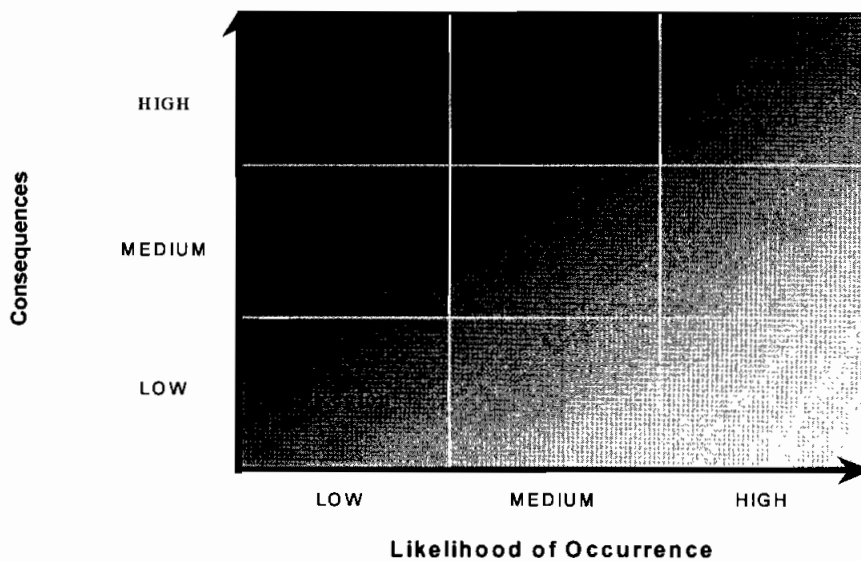
specific about the likelihood of an attack. One conclusion of this reasoning is that there is no risk – a potentially misleading and incorrect conclusion.

For this reason, surrogates to likelihood of attack are necessary. Due to the uncertainty of estimating the likelihood of an attack on any particular location, it is recommended to use several variables to compose an estimate. These are a function of an assumed threat, for example, a terrorist. For the purposes of a SVA, the definition of risk is:

***“Risk is an expression of the likelihood that a defined threat will target and successfully exploit a specific vulnerability of an asset and cause a given set of consequences.”<sup>9</sup>***

Figure 5.3 provides a simple depiction of risk, and Figure 5.4 defines risk for the SVA process.

**Figure 5.3—Example Risk Matrix**



**Figure 5.4—SVA Risk Definition**

<i>Security risk is a function of the consequences of an attack and the likelihood of the attack.</i>
<i>The likelihood of damage or loss of an asset is a function of the target's attractiveness, the degree of threat, and the degree of vulnerability to the attack.</i>

The risk variables are defined as shown in Figure 5.5.

<b>Figure 5.5—SVA Risk Variables<sup>10</sup></b>	
Consequences	Consequences are the potential impacts of the event.
Likelihood	The chance of being targeted for attack, and the conditional chance of mounting a successful attack (both planning and executing) given the threat and existing security measures. This is a function of the three variables below.
Threat	Threat is a function of the adversary intent, motivation, capabilities, and known patterns of potential adversaries. Different adversaries may pose different threats to various assets within a given facility.
Vulnerability	Vulnerability is a weakness that can be exploited by an adversary to gain access and damage or steal an asset or disrupt a critical function. This is a variable that indicates the likelihood of a successful attack given the intent to attack an asset.
Target Attractiveness	Target Attractiveness is a surrogate measure for likelihood of attack. This factor is a composite estimate of the perceived value of a target to the adversary and their degree of interest in attacking the target.

A high-risk event is represented by a high likelihood of a successful attack against a given critical target asset. Likelihood is determined by its attractiveness to the adversary, the degree of threat, and the degree of vulnerability. Criticality is determined by the asset's importance or value, and the potential consequences if attacked. If the likelihood of a successful attack is high, then the risk is considered high and appropriate countermeasures would be required for a high-risk asset.

For the SVA, the risk of the security event is estimated qualitatively. It is based on the consensus judgment of knowledgeable people as to how the likelihood and consequences of an undesired event scenario compares to other scenarios. The assessment is based on best available information, using experience and expertise to make sound risk management decisions. The company may use a risk matrix, which is a graphical representation of the risk factors, as a tool for risk assessment decisions.

#### **5.4.2 Consequences (C)**

The severity of the consequences of a security event at a facility is generally expressed in terms of the degree of injury or damage that would result if there was a successful attack. They may involve effects that are more severe than expected with accidental risk. Several examples of relevant consequences in a SVA include:

- Injuries to the public or to workers.
- Severe environmental damage (such as contamination of drinking water).
- Direct and indirect significant financial losses to the company.
- Disruption to the national, regional, or local operations and economy.
- Loss of business viability.

The estimate of consequences may be different in magnitude or scope than is normally anticipated for accidental releases. In the case of security events, adversaries are determined to maximize damage, so a worst case credible security event should be defined. Critical infrastructure may have dependencies and interdependencies that need careful consideration.

In addition, theft of hazardous materials should be included in SVAs as applicable. Terrorists may be interested in theft of hazardous materials to either cause direct harm at a later date or possibly to make chemical weapons using the stolen materials as constituents.

Consequences are used as one of the key factors in determining the criticality of the asset and the degree of security countermeasures required. During the initial screening, consequences and attractiveness are used to screen low value assets from further consideration.

#### **5.4.3 Threat (T)**

Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset.<sup>11</sup> It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Sources of threats may be categorized as:

- Terrorists (international or domestic),
- Activists, pressure groups, single-issue zealots,
- Disgruntled employees,
- Criminals (e.g., white collar, cyber hacker, organized, opportunists).

Adversaries may be categorized as occurring from three general groups:

- Insider threats,
- External threats,
- Insiders working as colluders with external threats.

Threat information is gathered and used during the SVA process as an important reference point. To assess an adversary's capability and intent, one must understand what may motivate them. A company should consider a range of threats and then look at their system's vulnerabilities to each type of threat. That assessment will determine the areas where an company will need additional help and information from federal, state, and local governments.

#### **5.4.4 Vulnerability (V)**

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and subsequent destruction or theft of an asset.<sup>12</sup> Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical security, or operational security practices. In a SVA, vulnerabilities are evaluated either by broadly considering the threat and hazards of the assets they could attack or affect, or analyzed by considering multiple potential specific sequences of events (a scenario-based approach).

#### **5.4.5 Target Attractiveness ( $A_T$ )**

Not all targets are of equal value to adversaries. A basic assumption of the SVA process is that target attractiveness is one factor that influences the likelihood of a security event. Target attractiveness is an estimate of the real or perceived value of a target to an adversary based on such factors as shown in Figure 5.6.

During the SVA, the attractiveness of each asset should be evaluated based on the adversary's intents or anticipated level of interest in the target if known. Security strategies can be developed around the estimated targets and potential threats.

<b>Figure 5.6—Target Attractiveness Factors</b>	
<b>Type of effect:</b>	
<ul style="list-style-type: none"> <li>• Potential for causing maximum casualties</li> <li>• Potential for causing maximum damage and economic loss to the facility and company</li> <li>• Potential for causing maximum damage and economic loss to the geographic region</li> <li>• Potential for causing maximum damage and economic loss to the national infrastructure</li> </ul>	
<b>Type of target:</b>	
<ul style="list-style-type: none"> <li>• Usefulness of the process material as a weapon to cause collateral damage</li> <li>• Proximity to a national asset or landmark</li> <li>• Difficulty of attack including ease of access and degree of existing security measures</li> <li>• High company reputation and brand exposure</li> <li>• Iconic or symbolic target</li> <li>• Chemical or biological weapons precursor chemical</li> <li>• Target recognition</li> </ul>	

## 5.5 Characteristics of a Sound SVA Approach

It is important to distinguish between a security risk management process and a SVA method. Security risk management is the overall process that includes the SVA, development and implementation of a security plan, and reintegration of data into subsequent SVAs. SVA is the estimation of risk for the purposes of decision-making. SVA methods may be very powerful analytical tools to integrate data and information, and help understand the nature and locations of risks of a system. However, SVA methods alone should not be relied upon to establish risk, nor solely determine decisions about how risks should be addressed. SVA methods should be used as part of a process that involves knowledgeable and experienced personnel that review the input, assumptions, and results. This review should integrate the SVA output with other factors, the impact of key assumptions, and the impact of uncertainties created by the absence of data or the variability in assessment inputs before arriving at decisions about risk and actions to reduce risk.

## 5.6 First Step in the SVA Process

After obtaining management approval and authorization to proceed, a typical first step in all SVA approaches is to collect a representative group of company experts, and outside experts if needed, to identify potential security related events or conditions, the consequences of these events, and the risk reduction activities for the company's system. These experts draw on the years of experience, practical knowledge, and observations from experienced field operations and maintenance personnel in understanding where the security risks may reside and what can be done about them. Such a company group typically consists of representation from: company security, risk management, operations, engineering, safety, environmental, regulatory compliance, logistics/distribution, IT and other team members as required. This group of experts will focus on the potential problems and risk control activities that would be effective in a facility security plan. The primary goal of this group is to capture and build into the SVA method the experience of this diverse group of individual experts so that the SVA process will capture and incorporate information that may not be available in typical operator databases.

There are a number of techniques employed by these expert teams that have proven useful in assuring a systematic and thorough review. These include:

- Free-form brainstorming of issues and potential risks.
- Conducting an asset-by-asset review.



- Using checklists or structured question sets designed to solicit information on a comprehensive list of potential risks and integrity issues, and
- Using simple risk matrices to qualitatively portray and communicate the likelihood and consequences of different security related events.

For each potential security threat or risk factor, the characteristics or variables that potentially could impact risk (both beneficially and adversely) are identified. During the SVA process, specific risk increasing characteristics of the system are either external variables (e.g., outside influences acting on the system), or operation variables (e.g., characteristics associated with the physical properties). In either case, these variables are features of the in-service system and are not easily altered. Variables should be considered individually based on how they impact a specific risk factor. This means that variables could be used in different ways and with potentially contradictory influences within the SVA.

## 5.7 SVA Strengths and Limitations

Each of the SVA methods commonly used has its strengths and limitations. Qualitative methods are well suited for making good sound security management decisions at the local asset level. In selecting an appropriate SVA method, there are a number of questions that should be considered. Some of the more significant ones are summarized below.

**Table 5.1—Questions to determine SVA Approach Needed**

<ul style="list-style-type: none"> <li>• Does the scope of the SVA method identify significant security related events and risks of the facility or along the system? If not, how can the risks that are not included in the SVA method be assessed and integrated in the future?</li> </ul>
<ul style="list-style-type: none"> <li>• Will all data be assessed, as it really exists along the system? Data should be location specific so that additive effects of the various risk variables can be determined. Can the assessment resolution be altered, e.g. station-by-station or mile-by-mile, dependent on the evaluation needs?</li> </ul>
<ul style="list-style-type: none"> <li>• Does the SVA method use numerical weights and other empirical factors to derive the risk measures and priorities? Are these weights based on the experience of the system, operator, industry, or external sources?</li> </ul>
<ul style="list-style-type: none"> <li>• Do the basic input variables of the SVA method require data that is available to the company? Do data systems and industry data updating procedures provide sufficient support to apply the SVA method effectively? What is the process for updating the SVA data to reflect changes in the system, the infrastructure, and new security related data? How is the input data validated to ensure that the most accurate, up-to-date depiction of the system is reflected in the SVA?</li> </ul>
<ul style="list-style-type: none"> <li>• Does the SVA output provide adequate support for the justification of risk-based decisions? Are the SVA results and output documented adequately to support justification of the decisions made using this output?</li> </ul>

## 5.8 Recommended Times for Conducting and Reviewing the SVA

Figure 5.7—Times for Conducting and Reviewing the SVA	
1	An initial review of all relevant facilities and assets per a schedule set by the an initial planning process
2	When an existing process or operation is proposed to be substantially changed and prior to implementation (revision or rework)
3	When a significant new process or operation is proposed and prior to implementation (revision or rework)
4	When the threat substantially changes, at the discretion of the owner/operator of the facility (revision or rework)
5	After a significant security incident, at the discretion of the owner/operator of the facility (revision or rework)
6	Periodically to revalidate the SVA (revision or rework)

## 5.9 Risk Control and Mitigation

SVA methods are also important tools to help owner/operators make cost effective and sound decisions to control security risks on their systems. Once a potential risk has been identified, SVA methods can be used to estimate the expected risk reduction or benefits that will be achieved. Potential capital and maintenance improvement activities may be prioritized to support management decision-making. This section provides an overview of this process.

After the results of the SVA are available, the next step is to examine the most significant risks on the system, as well as other opportunities to more efficiently control risks and determine what mitigation actions might be desirable. The risk control and mitigation process involves:

- Identification of risk control options that lower the likelihood of a security related event, reduce the consequences, or both, i.e., mitigation activities.
- A systematic evaluation and comparison of those options to quantify the risk reduction impact of the proposed project, and
- Selection and implementation of the optimum strategy for risk control.

Typically there are many ways to address a particular risk. For example, improvements or modifications can be made to the system hardware or equipment configuration, operation and maintenance practices, assessment practices, personnel training, control and monitoring methods, emergency response, and interface with the public and other external organizations. This guideline provides a discussion of risk control options that are frequently used to reduce different petroleum sector security risks. In order to find the optimum approach to risk control, it is important that a variety of options, and perhaps a combination of activities be considered rather than just taking the first idea that is proposed or doing what has always been standard practice. This allows management to consider innovative solutions and perhaps new technologies that may be more effective in addressing risk.

After identifying the risk control options available, the next step is to evaluate and compare the effectiveness of the different alternatives. This evaluation and comparison is often performed at more than one level. For example, a company may desire to select the best approach among several options to address a specific risk. In each case, the basis for comparison and ranking should consider both the magnitude of risk reduction benefits expected as well as the resources expended. Many owner/operators use a benefit-to-cost ratio where the benefit is the expected risk reduction to

evaluate and rank potential risk control projects. This can provide a simple, easy-to-understand metric that allows projects with diverse benefits to be compared.

When conducting a ranking of projects based on a benefit-to-cost approach, a comprehensive evaluation and comparison process should also include a review of the system risks to be sure that relatively high risks are not overlooked simply because the risk control projects proposed don't have a high benefit-to-cost ratio. This may signal the need to consider other risk control options.<sup>6</sup> The process should also consider the amount of risk reduction being achieved to be sure the most effective projects are being proposed. There are many other practical factors that are typically considered when evaluating and prioritizing activities. These can include:

- Uncertainties in both the risk reduction and cost estimates.
- Technological value of a particular option, e.g., employing a new security camera.
- Human resource and equipment constraints.
- Logistical and implementation issues, e.g., delay in ability of vendor to supply necessary equipment.
- Concerns of government organizations and other external constituencies.

When establishing a SVA program, an operator should consider the many features that are unique to its systems and operations to determine which approach is most appropriate. SVA is a "fact finding", not a "fault finding" system analysis. The ultimate goal of SVA is to identify and prioritize significant security risks in the system so the operator can determine how, where, and when to allocate risk mitigation resources to improve system security. The operator must decide what information could be useful in performing the assessment and how that information can be used to maximize the accuracy and effectiveness of the SVA.

### **5.10 Risk Screening**

Security issues potentially exist at every facility managed by the petroleum industry, but the threat of malevolent acts is likely to be differentiated across the industry. This is captured by the factor known as 'target attractiveness', whereby certain assets are considered to be more likely to be of interest to terrorists than others. Based on many reported threat assessments, intelligence reports, and actual events around the world, these factors can be used to evaluate target attractiveness.<sup>13</sup>

It is likely that most facilities have no specific threat history. A screening process may contain the following factors:

1. Target attractiveness or target value,
2. Degree of threat,
3. Difficulty of attack (function of adversary, current security and vulnerabilities),
4. Potential consequences (casualties, environmental, infrastructure and economic).

These are the same factors as are used for evaluating an individual asset risk, but the difference is that this is done at a generalized facility level for the risk screening.

Note that target attractiveness itself includes the other factors of consequences and difficulty of attack/vulnerability.

Arguably target attractiveness is the dominant factor in determining terrorist risk. Priority should be given to the Attractiveness Ranking when making assessments. In this way resources can be appropriately applied to assets where they are most likely to be important.

---

<sup>6</sup> Although summarized in a linear fashion for this guideline, the risk control and mitigation process, like the risk assessment process, can be highly iterative in nature.

## 6.0 Security Conditions and Potential Response Measures

This section describes a progressive level of protective measures that may be implemented in response to the possibility of a terrorist threat directed at a petroleum facility, facility assets, and personnel (including contractors) consistent with the Homeland Security Advisory System (HSAS) developed by the Department of Homeland Security. The purpose of the HSAS is to establish standardized alert and response measures for a broad range of threats and to help disseminate appropriate and timely information for the coordination and implementation of the response measures by management and operator personnel prior to and during a threat crisis. The associated response measures may be implemented for each security alert level at a facility.

In addition to HSAS, there are several other threat level systems used by both industry and other agencies. While the MARSEC levels utilize only a 3 Tier system, it may essentially be compared to HSAS with:

- MARSEC 1 equivalent to HSAS Green, Blue and Yellow.
- MARSEC 2 equivalent to HSAS Orange.
- MARSEC 3 equivalent to HSAS Red.

If a system other than HSAS or MARSEC has been implemented by an individual company it most likely has been developed based on HSAS, MARSEC or both and specific guidance contained below should be considered where appropriate.

Each company should be able to advise and communicate to company personnel and others as warranted the security condition at the facility. The potential measures associated with each alert level are not always prioritized but those implemented should be initiated concurrently where practical and as applicable. Facility management should maintain a record of specific actions taken for each alert level. Less attractive facilities, remote facilities, unmanned facilities may employ less stringent measures. Following is a detailed explanation for each alert level and the potential response measures associated with each level:

### 6.1 Low Condition—Green

This condition exists when there is a low risk of possible terrorist activity or civil unrest. **Green** condition is for normal operating conditions. All measures under **Green** should be maintained indefinitely. Potential measures to consider implementing include:

#### Access Control/Perimeter Protection

- Have all contractors and visitors check or sign in and out of the facility at designated location(s).
- Ensure existing security measures are in place and functioning such as fencing, locks, camera surveillance, intruder alarms, and lighting as appropriate.

#### Communications

- Establish emergency communications and contact information with appropriate agencies. Consider redundant emergency communications in both the hardware and the means for contacting agencies.

#### Training/Policies/Procedures/Plans

- Develop terrorist and security awareness information and provide relevant education to employees on security standards and procedures. Caution employees not to talk with outsiders concerning their facility or related issues.

- Advise all facility personnel to report the presence of unknown personnel, unidentified vehicles, aircraft or watercraft, vehicles, watercraft or aircraft operated out of the ordinary, abandoned packages, and other suspicious activities.
- Incorporate security awareness and information into public education programs and notifications to emergency response organizations as appropriate.
- Survey surrounding areas to determine those activities that might increase the security risks that could affect the facility (e.g., airports, government buildings, other industrial facilities).
- Ensure contingency and business continuity plans are current and include a response to terrorist threats.
- Review existing emergency response plans and modifying them, if required, in light of potential threats.

#### IT Security

- Develop and implement hardware, software, and communications security for computer-based operating systems.

### **6.2 Guarded Condition—Blue**

This condition exists when there is an increased general threat of possible terrorist activity against the facility or facility personnel, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of higher alert measures. It may be necessary to implement certain selected measures from higher alert levels to address information received or to act as a deterrent. All measures under **Blue** should be maintained as long as the **Blue** threat exists. In addition to the measures suggested by **Green**, the following measures could be considered:

#### Perimeter Protection/Access Control

- Secure all facilities, buildings and storage areas not in regular use, if possible. Increasing frequency of inspections and patrols within the facility, including the interior of buildings and along the facility perimeter.
- Inspect perimeter fencing and repairing all fence breakdowns. Review all outstanding maintenance and capital projects that could affect the security.
- Reduce the number of access points for and spot-check the contents of vehicles, aircraft, watercraft and personnel. Be alert to vehicles or watercraft parked or moored for an unusual length of time in or near a facility.
- Check designated unmanned sites at more frequent intervals for signs of unauthorized entry, suspicious packages, or unusual activities. Increase surveillance in designated areas.
- Require visitors to check in at a facility office and verifying their identification. Be especially alert to repeat visitors or outsiders who have no apparent business at the facility and are asking questions about the facility or the facility's personnel. Familiarizing facility personnel with vendors who service the facility and investigate unusual changes in vendor personnel.
- Inspect all packages/equipment coming into the facility. Do Not open suspicious packages. Consider reviewing the USPS "Suspicious Mail Alert" and the "Bombs by Mail" publications with all personnel involved in receiving packages.

#### Communications

- Inform personnel of the change in alert status. Review with employees the operations plans, personnel safety, and security details and logistic requirements that pertain to the increased security level. Implement procedures to provide periodic updates to employees on security measures being implemented that are considered confidential.
- Test security and emergency communications procedures and protocols as appropriate.

Training/Policies/Procedures/Plans

- Review all operations plans, personnel details, and logistics requirements that pertain to implementing higher alert levels.
- Review communications procedures and back-up plans with all concerned.

**6.3 Elevated Condition—Yellow**

This condition exists when there is an elevated risk of terrorist activity against the facility or facility personnel. All measures under **Yellow** should be maintained as long as the **Yellow** threat exists. In addition to the measures suggested by **Blue**, the following measures could be considered:

Perimeter Protection/Access Control

- Close and lock gates and barriers except those needed for immediate entry and egress. Inspect perimeter and perimeter fences on a regular basis. Ensure that other security systems are functioning and are available.
- Inspect on a more frequent basis the interior and exterior of all critical buildings and around all storage tanks and other designated critical areas.
- Dedicate personnel to assist with security duties to monitor personnel entering the facility and to inspecting the area on a regular basis, reporting to facility management as issues surface.
- Limit visitors and confirm that the visitor has a need to be and is expected at the facility. Escort visitors while at the facility pursuant to the specifics outlined in the security plan.

Communications

- Inform personnel of the change in alert status. Review with employees the operations plans, personnel safety, and security details and logistic requirements that pertain to the increased security level as appropriate. Implement procedures to provide periodic updates to employees on security measures being implemented.
- Check to ensure all emergency telephone, radio, and satellite communication devices are in place and they are operational.

Training/Policies/Procedures/Plans

- Confirm availability of security resources that assist with extended coverage.
- Identify areas where explosive devices could be potentially hidden.
- Instruct employees working alone to check-in on a periodic basis.

**6.4 High Condition—Orange**

This condition applies when there is a high risk of terrorist attacks or an incident occurs or information is received indicating that some form of terrorist action against the facility or facility personnel is imminent. Implementation of measures in this alert for more than a short period will probably create hardship and affect the routine activities of the facility and its personnel. In addition to the measures suggested for **Yellow**, the following measures could be considered:

Perimeter Protection/Access Control

- Reduce facility access points to the absolute minimum necessary for continued operation.
- Increase security patrol activity such as perimeter patrols and inspections.
- Check security systems such as lighting and intruder alarms to ensure they are functioning. Install additional, temporary lighting if necessary to adequately light all suspect areas or decreasing lighting to detract from the area.
- Prohibit unauthorized or unidentified vehicles/personnel entrance to the facility.

- Inspect vehicles entering the facility, including the cargo areas, undercarriage, glove boxes, and other areas where dangerous items could be concealed pursuant to the specifics outlined in the security plan. Inspect all packages and cargo being delivered by aircraft or watercraft in the same manner.
- Limit access to the facility to those personnel who have a legitimate and verifiable need to enter. Implementing positive identification of all personnel.

#### Communications

- Advise appropriate agencies that the facility is at an **Orange** alert level and advise of the measures being employed—requesting an increase in the frequency of their patrol of the facility.
- Consider consultation with local authorities about control of public roads and accesses by waterway that might make the facility more vulnerable to terrorist attack if they were to remain open.

#### Training/Policies/Procedures/Plans

- Continue **Green**, **Blue** and **Yellow** measures or introduce those that have not already been implemented.
- Develop procedures for shutting down and evacuation of the facility, if considered necessary, in case of imminent attack.
- Ensure that employees not work alone in remote areas or increasing the frequency of call-ins from remote locations.

### 6.5 Severe Condition—Red

This condition applies when there is a severe risk of terrorist attacks, an attack has occurred in the immediate area which may affect the facility, or when an attack is initiated on the facility and its personnel. Normally, this alert is declared as a localized condition at the facility. In addition to the measures suggested for **Orange**, the following measures could be considered:

#### Perimeter Protection/Access Control

- Augment security forces. Establish surveillance points and reporting criteria and procedures. Solicit assistance from appropriate agencies in securing the facility and access, if possible. Cooperate with authorities if they take control of security measures.

#### Training/Policies/Procedures/Plans

- Continue **Orange** and **Yellow** measures or introduce those that have not already been implemented.
- Consider shutting down the facility and operations in accordance with security contingency plans and evaluating security prior to resuming operations if they are temporarily shut down.
- Implement business contingency and continuity plans as appropriate.

## 7.0 Information (Cyber) Security

### 7.1 Introduction

The petroleum industry is a worldwide industry that is highly dependent on technology for its communications and operations. Technological advances that promote better efficiency and more automation within the petroleum industry also make information security an increasingly important issue. Technology is an important component of information security but without the integration of policies, procedures, processes and people, technology alone can not provide adequate information security.

It is widely understood that information security is important for office computing systems such as desktop PCs, laptops, servers, software programs, etc. What is less recognized is that computer technology has become pervasive throughout the entire organization, including network access to plant equipment to allow vendors to maintain systems remotely, and remote access connections to process control systems (SCADA) to allow engineers to trouble-shoot problems. In all of these environments, improper controls could allow unauthorized individuals to accidentally or intentionally harm the information assets of the petroleum industry.

To ensure that adequate and appropriate resources are allocated within the information security program, information security activities should be based on a thorough analysis of risks to the confidentiality, integrity and availability of the information assets. A comprehensive information technology security program implemented by member companies improves the security of the petroleum industry as a whole by effectively:

- Identifying and analyzing actual and potential precursor events that could result in cyber security-related incidents;
- Identifying the likelihood and consequence of potential cyber security-related events;
- Providing a comprehensive and integrated means for examining and comparing the spectrum of risks and risk reduction activities;
- Providing a structured, easily communicated means for selecting and implementing risk reduction activities;
- Monitoring program performance with the goal of improving that performance;
- Establishing alert and response measures for a broad range of security threats.

Additionally, the establishment of a communication program between federal agencies and the industry to share threat information also improves the security of the industry by providing an early warning mechanism so appropriate action can be taken in a timely manner.

ISO/IEC International Standard 17799, *Information technology—Code of practice for information security management*, describes a framework for creating an information security program and forms the basis of this guideline. ISO/IEC 17799 attempts to ensure preservation of confidentiality, integrity and availability of user access, hardware, software and data. The standard describes eight steps of an information security process: create an information security policy; select and implement appropriate controls; obtain upper management support; perform security vulnerability assessments (SVAs), create statements of applicability for all employees; create an information security management system; educate and train staff; and perform regular audits.

This framework has been endorsed by API's Information Technology Security Forum (ITSF) as voluntary guidance to protect the petroleum industry's information assets. The guidance contained herein and in ISO/IEC International Standard 17799 does not attempt to provide an all-inclusive list of information security considerations, but rather a framework for the evaluation and implementation of information security measures. The concepts mentioned in this Introduction are expounded upon in the following section.

## **7.2 Specific Security Guidelines**

### **7.2.1 Security Policies, Standards and Procedures**

Information Security policies, standards and procedures that focus on protecting a company's information technology assets are the foundation of a Security Management process. Policies are a prerequisite for defining the acceptable behaviors that a company desires to promote in protecting its critical information technology assets. Since policies set the tone for the company's culture relative to protecting information and information technology, a policy must have executive management



sponsorship, clearly articulate accountabilities and responsibilities, and be communicated to every employee and system user in the company. Company policies should address topics such as:

- Assignment of management responsibilities
- Business conduct and appropriate system use
- E-mail and internet use
- Remote access & third party connectivity
- System monitoring and compliance (audit)
- Physical security (laptops, computer rooms, etc)
- Incident reporting and response
- Data retention
- Business continuity and disaster recovery

The company Information Security Officer or Manager is generally accountable for the development, implementation and maintenance of a company's information security policies. However, it is recommended that this be accomplished by working in "partnership" with representatives from the functional areas of IT Audit, Human Resources, Legal, Corporate Security and Information Technology.

Each policy should be accompanied by a set of standards and procedures that provide guidance for the operational implementation and compliance assessment of the policies. The standards and procedures should be derived from industry technology standards and/or "best practices" and where appropriate, clearly define "mandatory" requirements to which adherence is not an option. Security policies should be tested from time to time to ensure adequate protections are in place. When new information assets are introduced, policies should be updated to reflect any changes that may be necessary.

### **7.2.2 Security Awareness and Education**

Companies should invest time and resources on an Information Security Awareness Program. To help safeguard company assets, employees must have the knowledge to understand the significance of their actions. A Security Awareness Program should designate responsibility for security training, clarify why security is important, identify who should attend Security Awareness Training, explain employee responsibilities, discuss existing security controls being taken to protect personnel and assets, and serve as a forum to discuss security questions.

Security awareness education should include "new hire" orientations, multi-media campaigns, and ongoing refresher activities. Incentive programs may also be utilized to bolster awareness and training efforts. Comprehensive security awareness programs will include both physical and cyber security initiatives.

### **7.2.3 Accountability and Ownership**

It is important to establish an owner for all policies, procedures, hardware, software and information assets. Having identifiable responsibility for these assets within a company is fundamental to the control process. The responsibility for many owner tasks can be delegated to custodians, but the owner remains accountable for the asset. Some of the key responsibilities of an owner include:

- Defining the business requirements for which the asset is needed,
- Establishing the value, criticality and sensitivity of the asset,
- Establishing, maintaining, documenting and verifying cost effective controls commensurate with the risk,

- Establishing policies and procedures to deal with issues related to the asset.

Since the business unit is typically in a better position to effectively assess business requirements, value, and sensitivity of an asset, it is recommended that ownership be placed within the business unit under most circumstances, not in the IT function. However, it would be appropriate for the IT function to own computing infrastructure and services that support the entire company, such as the company's network, etc.

#### **7.2.4 Data/Information Classification**

Information classification is the process of assigning protection categories or labels to information materials such as hardcopy documents and computer files. Classification of assets is generally based on the impact to the business if the information is lost, disclosed, corrupted or made unavailable. It is important to identify an organization's most critical information assets so that protection efforts and budget can be focused on those resources.

Typical components of a classification program include a policy that defines the classification program, identification of asset owners, definitions for various classifications, guidelines for handling, storing, transmitting and accessing information with various classifications, and an education program for employees. An information classification framework was developed by the API IT Security Forum. For more information call 202-682-8590.

#### **7.2.5 Security Vulnerability Assessments**

Security Vulnerability Assessments (SVA) are a cost-effective method to identify risks and reduce them to acceptable levels. SVAs should be performed on information technology assets on a routine basis to identify significant exposures that could lead to negative consequences. SVAs should evaluate the potential business and financial impacts of loss of information integrity, disclosure of sensitive information, loss of processing capability, violation of regulations, and the impact on health, safety or the environment. Key outcomes of an SVA are the documentation of the owner's judgment of exposures and risks in the absence of controls, and the documentation of follow-up action plans or the justification for accepting residual risks.

#### **7.2.6 Physical and Environmental Security**

It is important to prevent unauthorized access, theft or damage to computing systems and information assets. Critical or sensitive information processing equipment should be housed in secure facilities, protected by a defined security perimeter. The nature of this perimeter should be commensurate with the identified risks and value of the business assets. Protection should be extended to supporting facilities such as electrical supply and cabling infrastructure. Placement of systems should take into account environmental risks and should provide protection and detection from hazards such as fire. Policies should be implemented when feasible that require desks to be left clear of sensitive documents and media, and computer screens to be locked when unattended.

#### **7.2.7 Access Controls and Identity Management**

The implementation of appropriate access controls and the management of user identities are essential for the preservation of confidentiality, integrity and availability. These processes are typically applied to network, host, application and physical assets. The resulting audit trails should be monitored to detect anomalies.

Access control systems must allow authorized use of systems and resources, while preventing direct access by unauthorized users. Authorized users may be employees, contractors, third parties, or the

general public, but should be defined. Access controls include administrative controls such as policies, procedures, training, background checks and supervision; logical or technical controls such as passwords, two-factor authentication mechanisms, encryption, system hardening and protected protocols; and physical controls such as locks, cables, security cameras, guards and fences.

Identity Management or User Management systems maintain system user identities for the purpose of authenticating individuals to multiple systems. Identity management processes create, remove or modify an individual's access to systems in compliance with company policy. When an Identity Management system is functioning properly, a change to an individual's status will automatically and appropriately modify the access permitted to that individual throughout the environment.

### **7.2.8 Network Security**

Many controls are required to achieve and maintain the security of computer networks. Network controls should be implemented based on a clear policy that defines:

- The networks and network services which are allowed to be accessed.
- Authorization procedures for determining who is allowed to access which networks and networked services.
- Management controls and procedures to protect the access to network connections and network services.
- The degree of testing, monitoring and intrusion detection that is required to ensure required security levels are maintained.

Access to networks by remote users, access to network management facilities, and access to remote diagnostic ports on network equipment should require an appropriate level of authentication, such as two-factor authentication. Additional controls within the network to segregate information systems or groups of users should be considered when different levels of trust or security requirements exist. Shared networks and those linked to third parties require particular access control policies, traffic filtering, and routing controls to ensure that computer connections and information flows do not breach the access control policy of business applications. Security patches should be maintained on all network devices.

### **7.2.9 Systems Development**

Information security controls should be integrated into the initial phases of any application, data or system development process because it is much more effective to design information security requirements early in a development process rather than attempting to retrofit them after the system is operational. Security controls should be designed according to a risk mitigation strategy that attempts to reduce risk to levels acceptable to the business unit, based on the value of the asset and the likelihood of threats against it.

Periodic design reviews should be conducted during development and modification processes to assure that the design satisfies the specified security requirements. Production data should not be used to test application software until software integrity is assured. Application software should not be placed into production until the system tests have been successfully completed and the application has been properly certified and accredited. (See Change Control)

Infrastructure that supports applications that process or maintain sensitive data must be protected as well. Specific security controls such as intrusion detection/prevention and anti-virus should be implemented on hardware platforms and operating systems utilized during application development phases. Vulnerability assessment and patch management processes should be implemented to reduce or eliminate known or recently released vulnerabilities. Development and production environments

should be continuously monitored to verify controls such as identity management and access control are functioning as intended.

#### **7.2.10 Change Control**

It is important to establish a methodology to evaluate system changes and configuration controls to ensure the secure operation of the networking infrastructure and the continued confidentiality, integrity and availability of information systems. A change control process should be chartered and empowered to manage change within the information technology environment. This change control process should include features such as submission and evaluation of change requests, recovery and back-out procedures, and a mechanism to monitor and protect the organization's capacity to ensure uninterrupted availability.

#### **7.2.11 Viruses and other Malicious Code**

Increasingly complex and sophisticated malicious code continues to be prevalent, making it essential to implement effective controls to mitigate this risk. Recent versions of malicious code combine different infection techniques, carry new payloads, and steal or expose information rather than just destroying it. To reasonably mitigate this risk, multiple solutions should be deployed. Standard anti-virus software should be installed throughout the enterprise, on personal computers, data file servers, centralized application servers such as e-mail and web servers, and in the firewall complex. Anti-virus solutions should scan all protocols that could contain malicious code. To the extent possible, anti-virus software should be centrally administered to ensure desktops are updated quickly and uniformly.

Consideration should be given to the deployment of desktop (personal) firewalls and anti-spyware systems. Operating system and application security patches should be evaluated based on the risk they mitigate and installed as appropriate to reduce the effectiveness of malicious code. Finally, it is important to maintain employee awareness efforts since users are typically the first to receive malicious code and most often the cause of its distribution.

#### **7.2.12 Intrusion Detection and Incident Management**

Systems should be implemented and qualified personnel should be assigned to log and monitor inappropriate or unauthorized network activities. Electronic firewalls and other systems should be installed and configured to detect and prevent hostile activity at all external network access points, and between certain internal networks as appropriate. An incident response plan should be developed to ensure the timely and effective response to relevant exploits and report information of concern to appropriate Information Technology and business contacts, including internal public relations staff and government or law enforcement agencies. An incident response team should be assigned to respond to security events such as virus outbreaks, network penetration attempts, denial of service, intrusions and data theft or compromise. A computer security incident response plan was developed by the API IT Security Forum. For more information call 202-682-8590.

#### **7.2.13 Business Continuity, Business Resumption and Disaster Recovery**

Business Continuity, Business Resumption and Disaster Recovery are somewhat interchangeable terms. The intent of these plans is to enhance an organization's ability to counteract interruptions to normal operations. Business Impact Assessments should be performed by each department or function to determine the length of time they can operate without critical systems or processes before the business unit would incur a material loss. Appropriate business resumption plans, including well defined and tested data backup processes, should then be developed and implemented that would

have a reasonable probability of preventing such a material loss. These plans should be documented to form the Business Resumption Plan for the entire business unit. It is critical that Companies regularly test their Business Continuity Plans and revise the documentation as necessary to ensure the long-term effectiveness of their overall business continuity strategy.

#### **7.2.14 Regulatory Compliance**

Companies should establish a regulatory baseline to measure and provide corporate wide visibility to legal compliance requirements. To establish this baseline, all applications, systems and infrastructures should be identified and documented. Communication between corporate information security planners and other corporate functional sponsors or business owners should be established to ensure proper attention, visibility and guidance is obtained.

All relevant statutory, regulatory and contractual requirements should be identified, defined and documented for each information system. Major legislation has been passed in the following areas and should be addressed:

- Intellectual property (business information and copyrighted materials)
- Records retention (safeguard organizational records)
- Data protection and privacy of personal information
- Import/Export regulation (such as laws related to the use of encryption)
- Law enforcement (Rules of evidence)
- HIPPA, Sarbanes-Oxley, Graham-Leach-Bliley and others

#### **7.2.15 Audit (Compliance and Assurance)**

Security standards and policies can be very effective at safeguarding information assets and employees. However, in order to be effective, the standards and policies must be enforced. One way to ensure adequate protections are in place is by means of a standards compliance and assurance audit.

A company's executive management and Audit Committee have become increasingly interested in how well the company is protecting its critical information technology assets from unauthorized access and inappropriate use. One of the key assurance methods used by management is audit. Unsatisfactory audit reviews are discussed with management and/or the Audit Committee. These reviews typically require a clear definition of actions to be taken to prevent reoccurrence and a clear accountability for ensuring the actions are executed in a timely manner.

Other metrics that can be routinely evaluated and reported as indicators of the quality of health of the Information Security Management process and the associated policies, standards and procedures are the following:

- Appropriate use of Internet and e-mail systems
- Intrusion Detection reporting
- Password strength
- User account administration (modifications, additions, deletions)
- Change Management compliance

## Appendix A—Security Regulations Affecting the U.S. Petroleum Industry

Security Regulations Affecting the U. S. Petroleum Industry					
Operating Sector	Federal Agency	Issue	Requirement	Deadline	Authority References
Marine, Upstream, Downstream	USCG, DHS	Area Maritime Security Improvements – General Provision	Establishes framework for vessels and facilities located under, in, on or adjacent to U.S. waters to implement security plans developed under Parts 104, 105 and 106, to deter transportation security incidents, provides for civil and criminal penalties for noncompliance; provides for Coast Guard approval of Alternative Security Programs.		Final rule – 10/22/03 [68 FedReg 60448] 33 <i>CFR</i> Subchapter H, Part 101. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
	USCG, DHS	Area Maritime Security	Integrates port security-related requirements in the Maritime Transportation Security Act of 2002 with International Ship and Port Security Code (ISPS) and amendments to International Convention for Safety of Life at Sea (SOLAS). Establishes Area Maritime Security (AMS) Committee, directs the Committee to develop a risk-based AMS Assessment and an AMS Plan to respond to maritime security threats. (See J and K.)		Final rule – 10/22/03 [68 FedReg 60448] 33 <i>CFR</i> Subchapter H, Part 103. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
	USCG, DHS	Vessel Security	Requires owners or operators of vessels calling on U.S. ports to designate security officers for vessels, develop a Vessel Security Assessment, develop and submit to the USGS for approval a Vessel Security Plan that addresses components outlined in the rule, implement security measures specific to the vessel's operation, and comply with Maritime Security Levels. (See G.)	Plans to be submitted on or before 12/29/03. Compliance required on or before 6/30/04. Foreign vessels must have certificate of compliance with SOLAS and ISPS on or before 7/1/04.	Final rule – 10/22/03 [68 FedReg 60448] 33 <i>CFR</i> Subchapter H, Part 104. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
	USCG, DHS	Port Facility Security	Requires owners or operators of certain facilities at U.S. ports to designate security officers for facilities, develop a Facility Security Assessment, develop and submit to the USCG for approval a Facility Security plan that addresses components outlined in the rule, implement security measures specific to the facilities' operations, and comply with Maritime Security Levels. (See H.) See also updated regulations for handling of Class I (explosives) or other dangerous cargoes within or contiguous to waterfront facilities.	Plans to be submitted on or before 12/29/03. Compliance required on or before 6/30/04.	Final rule – 10/22/03 [68 FedReg 60448] 33 <i>CFR</i> Subchapter H, Part 105. See also Interim Final Rule 7/1/03 [68 FedReg 39240] Final Rule – 9/26/03 [68 FedReg 55436]
	USCG, DOT	Port/Facility Access: Identification Credentials	Clarifies the identification credentials that are acceptable to allow access to waterfront facilities and to port and harbor areas, including the vessels in them.	Clarification effective 9/6/02.	Clarification of Regulation – 8/7/02 [67 FedReg 51082] See also 33 <i>CFR</i> 6.10-5, 125.09(f), 125.15 and 125.53

**Security Regulations Affecting the U. S. Petroleum Industry**

<b>Operating Sector</b>	<b>Federal Agency</b>	<b>Issue</b>	<b>Requirement</b>	<b>Deadline</b>	<b>Authority References</b>
	USCG, DHS	Vessel Communication	Establishes technical and performance standards for an Automatic Identification System (AIS) and implements the AIS carriage requirements of the Maritime Transportation Security Act (MTSA) and the International Maritime Organization requirements adopted under International Convention for Safety of Life at Sea (SOLAS), 1974, as amended. Requires AIS on all vessels subject to SOLAS, Vessel Traffic Service Users and certain other commercial vessels. (See I and J.)	Varies by type of ship.	Final rule – 10/22/03 [68 FedReg 60448] 33 <i>CFR</i> Parts 26, 161, 164, 165. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
	USCG, DOT	Vessels: Notification of Arrival (NOA) in US Ports	For vessels bound for or departing US ports: Specifies information required in a NOA including additional crew and passenger information, consolidates and centralizes NOA submissions, requires earlier NOA submission times, provides exemptions for certain vessels, and creates exceptions to submission times for cargo declaration.	Requirements effective 4/1/03.	Final Rule – 2/28/03 [68 FedReg 9537]
<b>Upstream</b>	USCG, DHS	Outer Continental Shelf Facility Security	Requires certain offshore mobile drilling units and fixed oil and gas platforms to develop Facility Security Plans and Facility Security Assessment reports (See A, B, and E), designate security officers for OCS facilities, implement security measures specific to the facility's operation, and comply with Maritime Security Levels. Criteria based on production or number of personnel. Smaller facilities are not required to have assessments and plans but are encouraged to use industry standards such as API RP 70 (See F.) Coast Guard will review need for further security requirements and then consider separate rule making that would require compliance with industry standards.	Plans to be submitted on or before 12/29/03. Compliance required on or before 6/25/04. Facilities built after 7/1/04 must file for approval 60 days prior to beginning operations.	Final Rule – 10/22/03 [68 FedReg 60448] 33 <i>CFR</i> Subchapter H, Part 106. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
<b>Transportation</b>	RSPS, DOT	Hazmat transportation: Generally	Shippers and carriers of certain hazardous materials must develop and adhere to security plans. (See I.) Includes personnel security, unauthorized access information and en route security. Shippers and transporters of certain hazardous materials are required to comply with Federal security regulations that apply to motor carrier and vessel transportation.	Plans must be developed by 9/25/03. Compliance by 10/27/03.	Final rule – 3/25/03 [68 FedReg 14509] 49 <i>CFR</i> Part 172 Final rule – 9/26/03 [68 FedReg 55436] 33 <i>CFR</i> Part 126

Security Regulations Affecting the U. S. Petroleum Industry				
Operating Sector	Federal Agency	Issue	Requirement	Authority References
	RSPS, DOT	Hazmat transportation: Employee Training	Shippers and carriers of certain hazardous materials must ensure that employee training includes a security awareness component. In-depth training required for shippers which have security plans. See 3.1	Final rule -- 3/25/03 [68 FedReg 14509] Final rule -- 3/25/03 [68 FedReg 14509]
	FMCSA, DOT	Hazmat transportation: Employee security	Applicants for a commercial driver's license (CDL) to transport hazardous materials must pass a security screening/background check by the Transportation Security Administration. States required to change procedures for issuing licenses, including collecting fingerprints and biographical and criminal history information of applicants for a hazmat endorsement for a CDL. Security threat assessment standards established to review applicants for hazmat endorsement to commercial driver licenses (CDL). Appeal and waiver procedures established Certain individuals barred from shipping explosives. Exemption process provided.	Delay of compliance date -- 11/7/03 [68 FedReg 63030] Interim final rule -- 5/5/03 [68 FedReg 23844] 49 <i>CFR</i> Parts 383, 384 Delay of compliance date -- 11/7/03 [68 FedReg 63030] Interim final rule -- 5/5/03 [68 FedReg 23852] 49 <i>CFR</i> Parts 1570, 1572 Final rule -- 2/10/04 [69 FedReg 6195] Interim final rule -- 5/5/03 [68 FedReg 23832] 49 <i>CFR</i> 107.105(c) 18 USC 842, 845
	USCG, DHS	Hazmat transportation: Facility security	Requires improved security and procedures related to the handling of dangerous cargoes and to and from vessels at such facilities, including fire extinguishing equipment, fire appliances, warning signs, outdoor lighting, international shore connection meeting for facilities involved with foreign-flag vessels, limited personnel access, certified material handling and other vehicles, and adequate equipment, materials and standards. Applicable also to waterfront facilities.	Final rule -- 9/26/03 [68 FedReg 55436] 33 <i>CFR</i> 126



**Security Regulations Affecting the U. S. Petroleum Industry**

<b>Operating Sector</b>	<b>Federal Agency</b>	<b>Issue</b>	<b>Requirement</b>	<b>Deadline</b>	<b>Authority References</b>
	RSPS, FMCSA, DOT	Hazmat transportation: Security measures for motor carriers	Imposes specific security measures, e.g., escorts, vehicle tracing and monitoring systems, remote shutoffs, anti theft devices. Research and Special Programs Administration assumed the lead role from the Federal Motor Carrier Safety Administration for rulemaking addressing security of motor carrier shipments of hazardous materials.		ANPRM 7/16/02 [67 FedReg 46622] Notice -- 3/19/03 [698 FedReg 13250]
<b>Terminals</b>	FERC, USCG, OPS, RSPA, DOT	LNG Terminal Siting	Applications for authorization to build LNG terminals to FERC (land based) or Coast Guard (offshore) must include security assessment and security plan. (See O.)	With application.	Title 49 CFR Part 193, Subpart J -- Security 33 CFR Part 127
<b>Pipelines</b>	TSA, DHS	Security Assessment and Plan	OPS Pipeline Security Information Circular (non-public distribution) directs pipelines to identify critical facilities and develop, implement and annually review a security plan, utilizing industry association guidelines. OPS will audit to verify company response to circular. (See A, B, C, D and E.)	Written confirmation of compliance with the PSIC due 3/5/03.	Guidance with expectations and recommendations but not statutorily mandated. Pipeline Security Information Circular 9/5/02.
<b>All Sectors</b>	DHS	Procedures for handling Critical Infrastructure Information	Establishes procedures by which DHS will manage confidential data voluntarily submitted by companies. Implements Homeland Security Act of 2002 Sec. 214, also known as the Critical Infrastructure Act of 2002. Addresses how FOIA requests for physical and cyber vulnerability information will be handled.	Interim rule effective 2/20/04. Comments are due on 5/20/04	Interim rule -- 2/20/04 [69 FedReg 8074] 6 CFR 29.1 et seq. Proposed rule -- 4/15/03 [68 FedReg 18523]

**Statutory Authority:**

- Homeland Security Act of 2002—Signed into law 11/25/02. Public Law 107-296.
- Pipeline Safety Improvement Act of 2003—Signed into law 12/17/02. Public Law 107-355
- Maritime Transportation Security Act of 2002—Signed into law 11/25/02. Public Law 107-295
- USA PATRIOT Act—Signed into law 10/26/01. Public Law 107-56
- Safe Explosives Act—Signed into law 11/25/02. Public Law 107-296

## Appendix B—Glossary and Terms

**Adversary:** Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. An adversary could include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, rogue employees, and private interests. Adversaries can include site insiders, site outsiders, or the two acting in collusion.

**Alert Levels:** Describe a progressive, qualitative measure of the likelihood of terrorist actions, from negligible to imminent, based on government or company intelligence information. Different fixed or variable security measures may be implemented based on the level of threat to the facility.

**Asset:** An asset is any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets in the SVA include the community and the environment surrounding the site.

**Asset category:** Assets may be categorized in many ways. Among these are:

- Activities/Operations
- Environment
- Equipment
- Facilities
- Hazardous materials (used or produced)
- Information
- People

**Computer incident:** refers to an adverse event in an information system and/or network, or the threat of such an occurrence, which could cause loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples include: unauthorized use of another user's account, unauthorized use of system privileges, or execution of malicious code that destroys data. Adverse events such as natural disasters and power-related disruptions, though certainly undesirable incidents, are not generally within the scope of incident response teams and should be addressed in the business continuity (contingency) and Disaster Recovery plans. For the purpose of *Incident Response*, therefore, the term “computer incident” refers to an adverse event that is related to Information Security.

**Consequences:** The amount of loss or damage estimated to result from a successful attack against an asset. This should include consideration of casualties, facility damage, environmental impacts, and business interruption as appropriate.

**Control center:** A location from where a pipeline system is remotely monitored and operated. A control center is typically staffed on a 24/7 basis and is the location for continuous and centralized control of a pipeline system.

**Countermeasures:** An action taken or a physical capability provided whose principal purpose is to reduce or eliminate one or more vulnerabilities. The countermeasure may also affect the threat(s) (intent and/or capability) as well as the asset's value. The cost of a countermeasure may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

**Damage:** Impairment of the usefulness or value of information or computer resources (e.g., when a virus scrambles a file or makes a hard disk inoperable).

**Delay:** A countermeasures strategy that is intended to provide various barriers to slow the progress of an adversary in penetrating a site to prevent an attack or theft, or in leaving a restricted area to assist in apprehension and prevention of theft.

**Detection:** A countermeasures strategy to that is intended to identify an adversary attempting to commit a security event or other criminal activity in order to provide real-time observation as well as post-incident analysis of the activities and identity of the adversary.

**Deterrence:** A countermeasures strategy that is intended to prevent or discourage the occurrence of a breach of security by means of fear or doubt. Physical security systems such as warning signs, lights, uniformed guards, cameras, bars are examples of countermeasures that provide deterrence.

**Energy ISAC:** The Energy Information Sharing and Analysis Center is an industry organization that provides a secure database, analytic tools, and information gathering and distribution facilities designed to allow authorized individuals to submit either anonymous or attributed reports about information security threats, vulnerabilities, incidents and solutions.

**Event:** any observable occurrence in a system and/or network. Examples of events include the system boot sequence, a system crash and packet flooding within a network. Events sometimes provide indication that an incident is occurring. In reality, events caused by human error (e.g., unintentionally deleting a critical directory and all files contained therein) are the most costly and disruptive. Computer security-related events are attracting an increasing amount of attention among Information Security Professionals and within the general computing community.

**Hazard:** A situation with the potential for harm.

**Intelligence:** Information to characterize specific or general threats including the motivation, capabilities, and activities of adversaries.

**Intent:** A course of action that an adversary intends to follow.

**Likelihood of adversary success:** The potential for causing a catastrophic event by defeating the countermeasures. Likelihood of adversary success is an estimate that the security countermeasures will thwart or withstand the attempted attack, or if the attack will circumvent or exceed the existing security measures. This measure represents a surrogate for the conditional probability of success of the event.

**MOC (Management of Change):** An internal company management system to define, document, and communicate changes to a process as applicable.

**Operator:** A person or company who owns and/or operates petroleum facilities. For a person or company who owns or operates pipeline segments and/or facilities, the definition of operator is based on Title 49 *CFR* Part 195.

**Pipeline security plan:** Documentation that describes an operator's plan to address security issues and related events including security assessment and mitigation options and includes security condition levels and protective measures to security threats.

**Pipeline system:** Pipeline or pipeline segment and pipeline facilities such as a terminal, pump station, or other remote site plus the control center.

**Response:** The act of reacting to detected criminal activity either immediately following detection or post-incident via surveillance tapes or logs.

**Risk:** A measure of loss in terms of both the incident likelihood of occurrence and the magnitude of the consequences.

**Risk management:** An overall program consisting of: identifying potential threats to an area or equipment; assessing the risk associated with those threats in terms of incident likelihood and consequences; mitigating risk by reducing the likelihood, the consequences, or both; and measuring the risk reduction results achieved.

**Risk mitigation:** Those security measures employed at a facility to reduce the security risk to that facility.

**Safeguard:** Any device, system or action that either would likely interrupt the chain of events following an initiating event or that would mitigate the consequences.<sup>1</sup>

**SCADA:** Supervisory Control and Data Acquisition used for the remote control and monitoring of a pipeline system

**Security plan:** A document that describes an operator's plan to address security issues and related events including security assessment and mitigation options and includes security alert levels and response measures to security threats.

**Security risk management:** An overall plan consisting of: identifying potential security threats to pipeline segments and facilities; assessing the risks associated with those threats in terms of incident likelihood and consequences; mitigating the risk by reducing the likelihood, the consequences, or both; and evaluating the risk reduction results achieved.

**Security risk mitigation:** Those security measures employed on a pipeline system to reduce the security risk to the pipeline system.

**Security Vulnerability Assessment (SVA):** A systematic, analytical process in which potential security threats and vulnerabilities to facility or system operations are identified and the likelihood and consequences of potential adverse events are determined. SVAs can have varying scopes and can be performed at varying levels of detail depending on the operator's objectives - see Section 5.

**Segment:** an aspect of the petroleum industry that represent one of the steps needed to find, produce, process and transport petroleum from where they are found deep below the earth's surface to where they will be consumed. For purposes of this guidance document, the petroleum segments are defined as petroleum exploration and production (Upstream), petroleum refining, pipeline transportation (liquids), marine transportation, and petroleum products distribution and marketing.

**Should:** The term "should" is used in this document to indicate those practices which are preferred, but for which Owner/Operators may determine that alternative practices are equally or more effective or those practices for which engineering judgment is required.

**Terrorism:** "The unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives" - (FBI).

**Threat:** Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

***Threat categories:*** Adversaries may be categorized as occurring from three general areas:

- Insiders
- Outsiders
- Insiders working in collusion with outsiders

***Vulnerability:*** Any weakness that can be exploited by an adversary to gain access to and damage or steal an asset. Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings, or operational and personnel practices.

## **Appendix C—Communication of Security Intelligence**

One important key to mitigate acts of terror and to protect facilities is good intelligence, and the quick dissemination of information to the large number of Owner/Operators that may need the information.

Information Sharing and Analysis Centers (ISACs) were created to serve as information dissemination organizations to provide government intelligence to industry concerning potential acts of terrorism. An ISAC consists of a secure database, analytic tools, and information gathering and distribution facilities that allow authorized individuals to submit either anonymous or attributed reports about information and physical security threats, vulnerabilities, incidents, and solutions. ISAC members also have access to information and analysis related to information provided by other members and obtained from other sources, such as the US government and law enforcement agencies, technology providers, and security associations such as CERT. The ENERGY-ISAC is exclusively for, and designed by, professionals in the energy industries. No U.S. government agency, regulator, or law enforcement agency can access the ENERGY-ISAC. Other critical industries, such as finance and telecommunications, also have ISACs in place.

Organizations wishing to apply for membership in the ISAC may obtain membership information at (<http://www.energyisac.com/>) or by calling 202-682-8286. Membership requests should be mailed to the ISAC administrator at:

<p><b>ENERGY-ISAC</b> <b>1220 L. Street N.W., Suite 900</b> <b>Washington, D.C. 20005</b> <b>USA</b></p>
--

## Appendix D—References

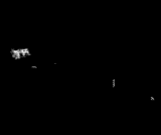
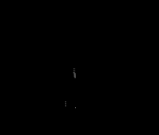
- <sup>1</sup> American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS) “Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites”, August, 2002.
- <sup>2</sup> “The Sociology And Psychology Of Terrorism: Who Becomes A Terrorist And Why?,” A Report Prepared under an Interagency Agreement by the Federal Research Division, Rex A. Hudson, et. al. Library of Congress, September, 1999.
- <sup>3</sup> “Patterns of Global Terrorism” 2001, May, 2002, U. S. State Department.
- <sup>4</sup> Testimony Before the Senate Committee on Governmental Affairs, United States General Accounting Office, October 31, 2001, “A Risk Management Approach Can Guide Preparedness Efforts”, Statement of Raymond J. Decker, Director, Defense Capabilities and Management.
- <sup>5</sup> CCPS, 2002.
- <sup>6</sup> The National Infrastructure Protection Center, “Suggested Guidance on Protective Measures,” Information Bulletin 03-002, February 7, 2003.
- <sup>7</sup> COMDTPUB P 16700.4, U.S. DOT, USCG, NVIC 11-02, 13 January 2003.
- <sup>8</sup> American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS) “Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites”, August, 2002.
- <sup>9</sup> Ibid, AIChE.
- <sup>10</sup> Ibid, AIChE.
- <sup>11</sup> Ibid, AIChE.
- <sup>12</sup> Ibid, AIChE.
- <sup>13</sup> “National Infrastructure Protection Center, Homeland Security Information Update, Potential Al-Qa’ida Operational Planning,” Information Bulletin 03-001, February 7, 2003.











**Petroleum Refineries**

**Liquid Petroleum Pipelines**

**Petroleum Products Distribution and Marketing**

**Oil and Natural Gas Production Operations**

**Marine Transportation**

**Cyber/Information Technology for the Petroleum Industry**

Additional copies are available through Global Engineering Documents at 1-800-854-7179 or 303-397-7956.

Information about API Publications, Programs and Services is available on the web at [www.api.org](http://www.api.org).

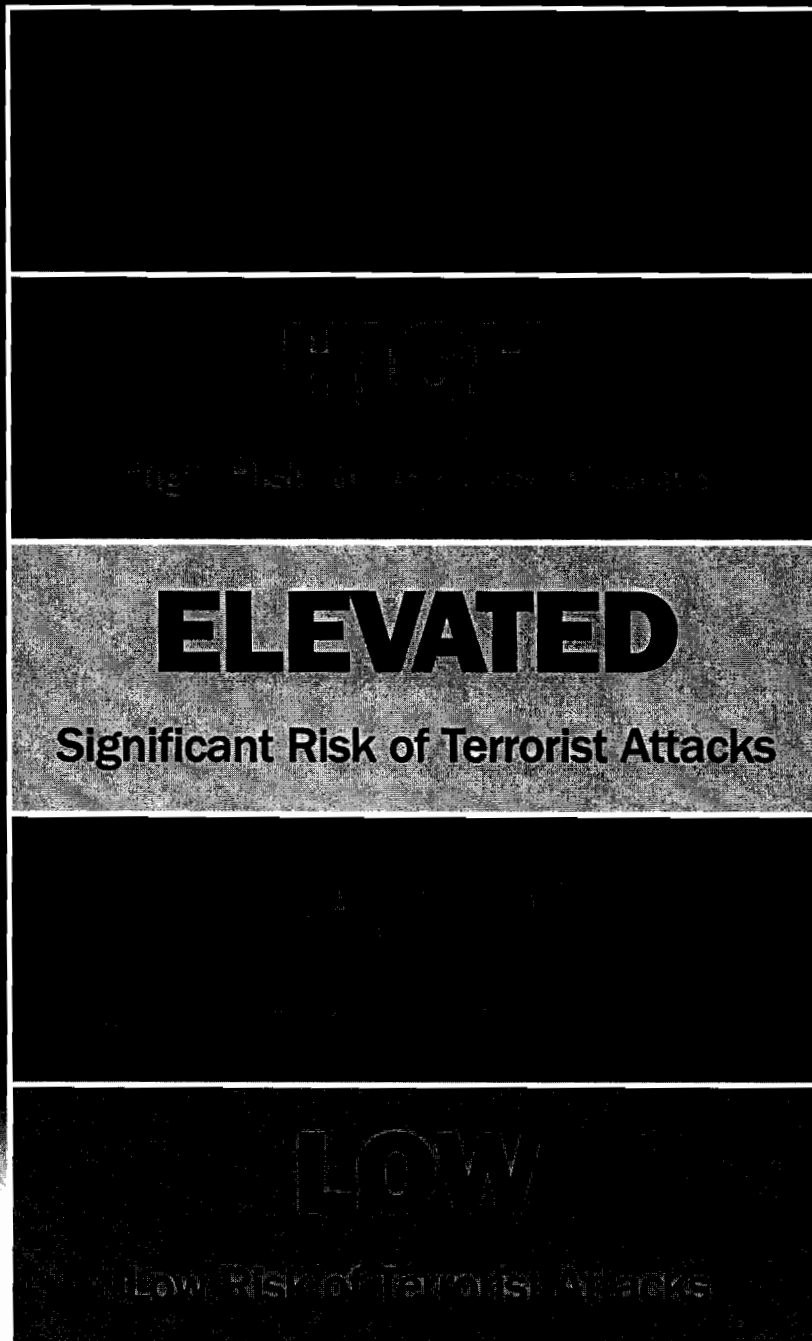
**API**<sup>®</sup>

American Petroleum Institute

1220 L Street, NW  
Washington, DC 20005-4070  
USA  
202-682-8000

Product No. OS0002

# Homeland Security Advisory System



[www.dhs.gov](http://www.dhs.gov)

Third Edition

Petroleum  
Refineries

Liquid  
Petroleum  
Pipelines

Petroleum  
Products  
Distribution  
and Marketing

Oil and  
Natural Gas  
Production  
Operations

Marine  
Transportation

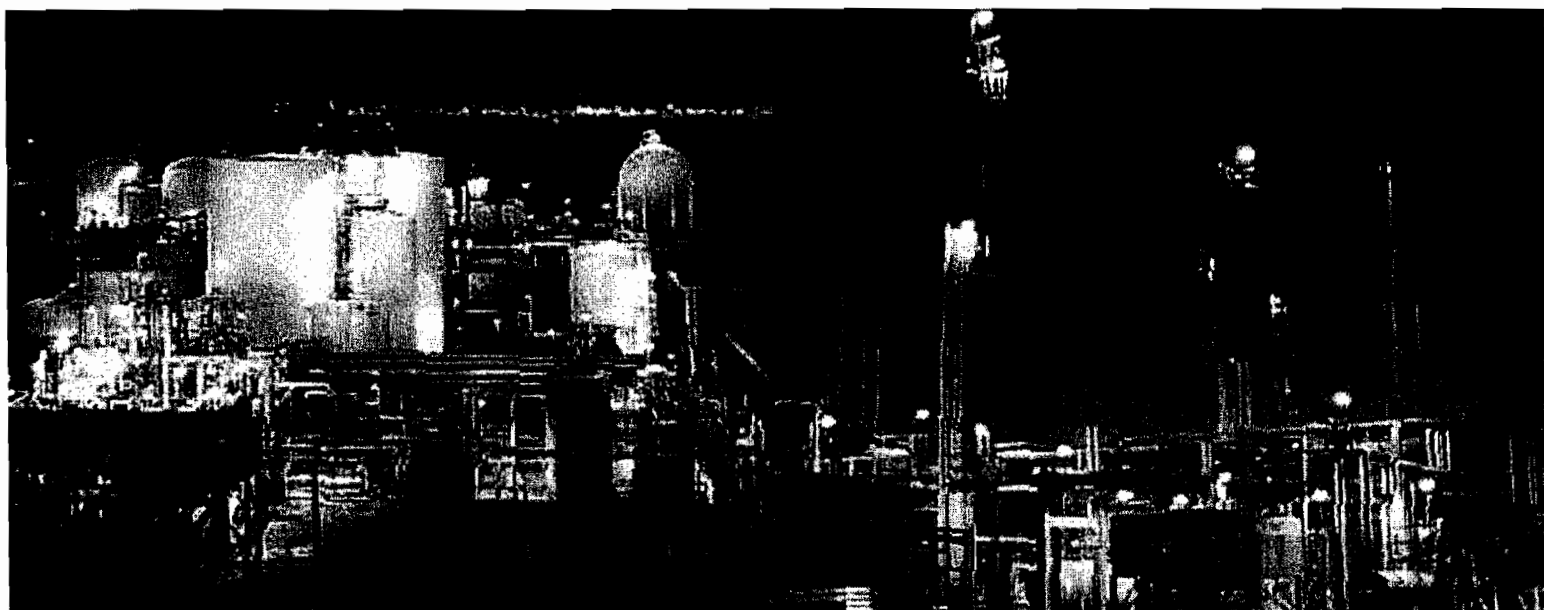
Cyber/  
Information  
Technology for  
the Petroleum  
Industry


# Security Guidelines for the Petroleum Industry

American Petroleum Institute  
April 2005

October 2004

Security Vulnerability Assessment  
Methodology for the Petroleum and  
Petrochemical Industries, Second Edition



 American  
Petroleum  
Institute

  
NPRA

October 2004

**Security Vulnerability Assessment  
Methodology for the Petroleum and  
Petrochemical Industries, Second Edition**

American Petroleum Institute  
1220 L Street, NW  
Washington, DC  
20005-4070

National Petrochemical &  
Refiners Association  
1899 L Street, NW  
Suite 1000  
Washington, DC  
20036-3896

All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 1220 L Street, N.W., Washington, D.C. 20005.

*Copyright © 2004 American Petroleum Institute*



## PREFACE

The American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) are pleased to make this Second Edition of this Security Vulnerability Assessment Methodology available to members of petroleum and petrochemical industries. The information contained herein has been developed in cooperation with government and industry, and is intended to provide a tool to help maintain and strengthen the security of personnel, facilities, and industry operations; thereby enhancing the security of our nation's energy infrastructure.

API and NPRA wish to express sincere appreciation to the member companies who have made personnel available to work on this document. We especially thank the Department of Homeland Security and its Directorate of Information Analysis & Infrastructure Protection and the Department of Energy's Argonne National Laboratory for their invaluable contributions. The lead consultant in developing this methodology has been David Moore of the AcuTech Consulting Group, whose help and experience was instrumental in developing this document. Lastly, we want to acknowledge the contributions of the Centers for Chemical Process Safety for their initial work on assessing security vulnerability in the chemical industry.

This methodology constitutes but one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities. However, there are several other vulnerability assessment techniques and methods available to industry, all of which share common risk assessment elements. Many companies, moreover, have already assessed their own security needs and have implemented security measures they deem appropriate. This document is not intended to supplant measures previously implemented or to offer commentary regarding the effectiveness of any individual company efforts.

The focus of this second edition was to expand the successful first edition by including additional examples of how the methodology can be applied to a wide range of assets and operations. This includes petroleum refining and petrochemical manufacturing operations, pipelines, and transportation including truck and rail. The methodology was originally field tested at two refinery complexes, including an interconnected tank farm, marine terminal and lube plant before the publication of the first edition. Since then, it has been used extensively at a wide variety of facilities involving all aspects of the petroleum and petrochemical industries.

API and NPRA are not undertaking to meet the duties of employers, manufacturers, or suppliers to train and equip their employees, nor to warn any who might potentially be exposed, concerning security risks and precautions. Ultimately, it is the responsibility of the owner or operator to select and implement the security vulnerability assessment method and depth of analysis that best meet the needs of a specific location.



## CONTENTS

CHAPTER 1 INTRODUCTION .....	1
1.1 INTRODUCTION TO SECURITY VULNERABILITY ASSESSMENT.....	1
1.2 OBJECTIVES, INTENDED AUDIENCE AND SCOPE OF THE GUIDANCE .....	1
1.3 SECURITY VULNERABILITY ASSESSMENT AND SECURITY MANAGEMENT PRINCIPLES.....	2
CHAPTER 2 SECURITY VULNERABILITY ASSESSMENT CONCEPTS .....	3
2.1 INTRODUCTION TO SVA TERMS .....	3
2.2 RISK DEFINITION FOR SVA .....	3
2.3 CONSEQUENCES .....	4
2.4 ASSET ATTRACTIVENESS .....	4
2.5 THREAT.....	5
2.6 VULNERABILITY .....	5
2.7 SVA APPROACH.....	5
2.8 CHARACTERISTICS OF A SOUND SVA APPROACH .....	7
2.9 SVA STRENGTHS AND LIMITATIONS .....	8
2.10 RECOMMENDED TIMES FOR CONDUCTING AND REVIEWING THE SVA.....	8
2.11 VALIDATION AND PRIORITIZATION OF RISKS.....	8
2.12 RISK SCREENING .....	9
CHAPTER 3 SECURITY VULNERABILITY ASSESSMENT METHODOLOGY .....	9
3.1 OVERVIEW OF THE SVA METHODOLOGY .....	9
3.2 SVA METHODOLOGY .....	15
3.3 STEP 1: ASSETS CHARACTERIZATION.....	18
3.4 STEP 2: THREAT ASSESSMENT.....	23
3.5 SVA STEP 3: VULNERABILITY ANALYSIS .....	25
3.6 STEP 4: RISK ANALYSIS/RANKING .....	28
3.7 STEP 5: IDENTIFY COUNTERMEASURES:.....	28
3.8 FOLLOW-UP TO THE SVA.....	29
ATTACHMENT 1 – EXAMPLE SVA METHODOLOGY FORMS .....	31
ABBREVIATIONS AND ACRONYMS .....	41
APPENDIX A—SVA SUPPORTING DATA REQUIREMENTS .....	43
APPENDIX B—SVA COUNTERMEASURES CHECKLIST .....	45
APPENDIX C—SVA INTERDEPENDENCIES AND INFRASTRUCTURE CHECKLIST.....	67
APPENDIX C1—REFINERY SVA EXAMPLE .....	115
APPENDIX C2—PIPELINE SVA EXAMPLE .....	123
APPENDIX C3—TRUCK TRANSPORTATION SVA EXAMPLE .....	135
APPENDIX C4—RAIL TRANSPORTATION SVA EXAMPLE .....	145
References .....	155
Figures	
2.1 Risk Definition .....	3
2.2 SVA Risk Variables .....	3
2.3 Asset Attractiveness Factors .....	4
2.4 Overall Asset Screening Approach.....	6
2.5 Recommended Times for Conducting and Reviewing the SVA .....	9

3.1	Security Vulnerability Assessment Methodology Steps .....	11
3.1a	Security Vulnerability Assessment Methodology—Step 1 .....	12
3.1b	Security Vulnerability Assessment Methodology—Step 2.....	13
3.1c	Security Vulnerability Assessment Methodology—Steps 3 – 5 .....	14
3.2	SVA Methodology Timeline .....	15
3.3	SVA Team Members .....	16
3.4	Sample Objectives Statement .....	16
3.5	Security Events of Concern .....	17
3.6	Description of Step 1 and Substeps .....	19
3.7	Example Candidate Critical Assets .....	20
3.8	Possible Consequences of Security Events .....	21
3.9	Example Definitions of Consequences of the Event.....	22
3.10	Description of Step 2 and Substeps .....	23
3.11	Threat Rating Criteria.....	25
3.12	Target Attractiveness Factors (for Terrorism) .....	25
3.13	Attractiveness Factors Ranking Definitions (A).....	26
3.14	Description of Step 3 and Substeps .....	26
3.15	Vulnerability Rating Criteria .....	27
3.16	Description of Step 4 and Substeps .....	28
3.17	Risk Ranking Matrix .....	29
3.18	Description of Step 5 and Substeps .....	29
A	SVA Methodology Flow Diagram .....	124

# Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries

## Chapter 1 Introduction

### 1.1 INTRODUCTION TO SECURITY VULNERABILITY ASSESSMENT

The first step in the process of managing security risks is to identify and analyze the threats and the vulnerabilities facing a facility by conducting a Security Vulnerability Assessment (SVA). The SVA is a systematic process that evaluates the likelihood that a threat against a facility will be successful. It considers the potential severity of consequences to the facility itself, to the surrounding community and on the energy supply chain.

The SVA process is a team-based approach that combines the multiple skills and knowledge of the various participants to provide a complete security analysis of the facility and its operations. Depending on the type and size of the facility, the SVA team may include individuals with knowledge of physical and cyber security, process safety, facility and process design and operations, emergency response, management and other disciplines as necessary.

The objective of conducting a SVA is to identify security hazards, threats, and vulnerabilities facing a facility, and to evaluate the countermeasures to provide for the protection of the public, workers, national interests, the environment, and the company. With this information security risks can be assessed and strategies can be formed to reduce vulnerabilities as required. SVA is a tool to assist management in making decisions on the need for countermeasures to address the threats and vulnerabilities.

### 1.2 OBJECTIVES, INTENDED AUDIENCE AND SCOPE OF THE GUIDANCE

This document was prepared by the American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) Security Committees to assist the petroleum and petrochemical industries in understanding security vulnerability assessment and in conducting SVAs. The guidelines describe an approach for assessing security vulnerabilities that is widely applicable to the types of facilities operated by the industry and the security issues they face. During the development process it was field tested at two refineries, two tank farms, and a lube plant, which included typical process equipment, storage tanks, marine operations, infrastructure, pipelines, and distribution terminals for truck and rail. Since then, it has been used extensively at a wide variety of facilities involving all aspects of the petroleum and petrochemical industry.

This methodology constitutes one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities. However, there are several other vulnerability assessment techniques and methods available to industry, all of which share common risk assessment elements. Many companies, moreover, have already assessed their own security needs and have implemented security measures they deem appropriate. This document is not intended to supplant measures previously implemented or to offer commentary regarding the effectiveness of any individual company efforts.

Ultimately, it is the responsibility of the owner/operator to choose the SVA method and depth of analysis that best meets the needs of the specific location. Differences in geographic location, type of operations, and on-site quantities of hazardous substances all play a role in determining the level of SVA and the approach taken. Independent of the SVA method used, all techniques include the following activities:

- Characterize the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure;
- Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each adversary and the consequences if they are damaged or stolen;
- Identify potential security vulnerabilities that threaten the asset's service or integrity;
- Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur;
- Rank the risk of the event occurring and, if high risk, make recommendations for lowering the risk;
- Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses) and re-assess risk to ensure adequate countermeasures are being applied.

This guidance was developed for the industry as an adjunct to other available references which includes:

- American Petroleum Institute, "Security Guidelines for the Petroleum Industry", May, 2003;
- API RP 70, "Security for Offshore Oil and Natural Gas Operations", First Edition, April, 2003;

- “Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites”, American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), August, 2002;
- “Vulnerability Analysis Methodology for Chemical Facilities (VAM-CF)”, Sandia National Laboratories, 2002.

API and NPRA would like to acknowledge the contribution of the Center for Chemical Process Safety (CCPS) compiled in their “Guidelines for Analyzing and Managing the Security of Fixed Chemical Sites.” It was this initial body of work that was used as a basis for developing the first edition of the API NPRA SVA methodology. Although similar in nature, the SVA Method was developed for the petroleum and petrochemical industry, at both fixed and mobile systems. Examples have been added that demonstrate applicability at various operating segments of the industry. Owner/Operators may want to use any of the methods above, or another equivalent and appropriate methodology in conducting their SVAs. These guidelines should also be considered in light of any applicable federal, state and local laws and regulations.

The guidance is intended for site managers, security managers, process safety managers, and others responsible for conducting security vulnerability analyses and managing security at petroleum and petrochemical facilities.

The method described in this guidance may be widely applicable to a full spectrum of security issues, but the key hazards of concern are malevolent acts, such as terrorism, that have the potential for widespread casualties or damage.

These guidelines provide additional industry segment specific guidance to the overall security plan and SVA method presented in Part I of the API Security Guidelines for the Petroleum Industry.

### 1.3 SECURITY VULNERABILITY ASSESSMENT AND SECURITY MANAGEMENT PRINCIPLES

Owner/Operators should ensure the security of facilities and the protection of the public, the environment, workers, and the continuity of the business through the management of security risks. The premise of the guidelines is that security risks should be managed in a risk-based, performance-oriented management process.

The foundation of the security management approach is the need to identify and analyze security threats and vulnerabilities, and to evaluate the adequacy of the countermeasures provided to mitigate the threats. Security Vulnerability Assessment is a management tool that can be used to assist in accomplishing this task, and to help the owner/operator in making decisions on the need for and value of enhancements.

The need for security enhancements will be determined partly by factors such as the degree of the threat, the degree of vulnerability, the possible consequences of an incident, and the attractiveness of the asset to adversaries. In the case of terrorist threats, higher risk sites are those that have critical importance, are attractive targets to the adversary, have a high level of consequences, and where the level of vulnerability and threat is high.

SVAs are not necessarily a quantitative risk assessment, but are usually performed qualitatively using the best judgment of the SVA Team. The expected outcome is a qualitative determination of risk to provide a sound basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures.

A basic premise is that all security risks cannot be completely prevented. The security objectives are to employ four basic strategies to help minimize the risk:

1. Deter
2. Detect
3. Delay
4. Respond

Appropriate strategies for managing security can vary widely depending on the individual circumstances of the facility, including the type of facility and the threats facing the facility. As a result, this guideline does not prescribe security measures but instead suggests means of identifying, analyzing, and reducing vulnerabilities. The specific situations must be evaluated individually by local management using best judgment of applicable practices. Appropriate security risk management decisions must be made commensurate with the risks. This flexible approach recognizes that there isn't a uniform approach to security in the petroleum industry, and that resources are best applied to mitigate high-risk situations primarily.

All Owner/Operators are encouraged to seek out assistance and coordinate efforts with federal, state, and local law enforcement agencies, and with the local emergency services and Local Emergency Planning Committee. Owner/Operators can also obtain and share intelligence, coordinate training, and tap other resources to help deter attacks and to manage emergencies.

## Chapter 2 Security Vulnerability Assessment Concepts

### 2.1 INTRODUCTION TO SVA TERMS

A Security Vulnerability Assessment (SVA) is the process that includes determining the likelihood of an adversary successfully exploiting vulnerability and estimating the resulting degree of damage or impact. Based on this assessment, judgments can be made on degree of risk and the need for additional countermeasures. To conduct a SVA, key terms and concepts must be understood as explained in this chapter.

### 2.2 RISK DEFINITION FOR SVA

For the purposes of a SVA, the definition of risk is shown in Figure 2.1. The risk that is being analyzed for the SVA is defined as an expression of the likelihood that a defined threat will target and successfully attack a specific security vulnerability of a particular target or combination of targets to cause a given set of consequences. The complete SVA may evaluate one or more issues or sum the risk of the entire set of security issues. The risk variables are defined as shown in Figure 2.2.

A high-risk event, for example, is one which is represented by a high likelihood of a successful attack against a given critical target asset. Likelihood is determined by considering several factors including its attractiveness to the adversary, the degree of threat, and the degree of vulnerability. Criticality is determined by the asset's importance or value, and the potential consequences if attacked. If the likelihood of a successful attack against an important asset is high, then the risk is considered high and appropriate countermeasures would be required for a critical asset at high risk.

For the SVA, the risk of the security event is normally estimated qualitatively. It is based on the consensus judgment of a team of knowledgeable people as to how the likelihood and consequences of an undesired event scenario compares to other scenarios. The assessment is based on best available information, using experience and expertise of the team to make sound risk management decisions. The team may use a risk matrix, which is a graphical representation of the risk factors, as a tool for risk assessment decisions.

The API NPRA SVA Methodology has a two step screening process to focus attention on higher risk events. The key variables considered in the first screening are Consequences and Target Attractiveness. If either of those are either not sufficiently significant, the asset is screened out from further specific consideration. Later, the complete set of risk variables shown in Figure 2.1 are used in the second screen to determine the need for additional specific countermeasures.

Figure 2.1—Risk Definition

<b>Security Risk</b> is a function of:	
<ul style="list-style-type: none"> <li>• <b>Consequences</b> of a successful attack against an asset and</li> <li>• <b>Likelihood</b> of a successful attack against an asset.</li> </ul>	
<b>Likelihood</b> is a function of:	
<ul style="list-style-type: none"> <li>• the <b>Attractiveness</b> to the adversary of the asset,</li> <li>• the degree of <b>Threat</b> posed by the adversary, and</li> <li>• the degree of <b>Vulnerability</b> of the asset.</li> </ul>	

Figure 2.2—SVA Risk Variables<sup>4</sup>

Consequences	<i>Consequences</i> are the potential adverse impacts to a facility, the local community and/or the nation as a result of a successful attack.
Likelihood	<i>Likelihood</i> is a function of the chance of being targeted for attack, and the conditional chance of mounting a successful attack (both planning and executing) given the threat and existing security measures. This is a function of Threat, Vulnerability, and Target Attractiveness (see Figure 2.1).
Attractiveness	<i>Attractiveness</i> is a surrogate measure for likelihood of attack. This factor is a composite estimate of the perceived value of a target to a specific adversary.
Threat	<i>Threat</i> is a function of an adversary's intent, motivation, capabilities, and known patterns of operation. Different adversaries may pose different threats to various assets within a given facility or to different facilities.
Vulnerability	<i>Vulnerability</i> is any weakness that can be exploited by an adversary to gain access and damage or steal an asset or disrupt a critical function. This is a variable that indicates the likelihood of a successful attack given the intent to attack an asset.

<sup>4</sup>Ibid, AIChE.

## 2.3 CONSEQUENCES

The severity of the consequences of a security event at a facility is generally expressed in terms of the degree of injury or damage that would result if there were a successful attack. Malevolent acts may involve effects that are more severe than expected with accidental risk. Some examples of relevant consequences in a SVA include:

- Injuries to the public or to workers.
- Environmental damage.
- Direct and indirect financial losses to the company and to suppliers and associated businesses.
- Disruption to the national economy, regional, or local operations and economy.
- Loss of reputation or business viability.
- Need to evacuate people living or working near the facility.
- Excessive media exposure and related public concern affecting people that may be far removed from the actual event location.

The estimate of consequences may be different in magnitude or scope than is normally anticipated for accidental releases. In the case of security events, adversaries are determined to cause maximize damage, so a worse credible security event should be defined. Critical infrastructure especially may have dependencies and interdependencies that need careful consideration.

In addition, theft of hazardous materials should be included in SVAs as applicable. Adversaries may be interested in theft of hazardous materials to either cause direct harm at a later date, use them for other illicit purposes such as illegal drug manufacturing, or possibly to make chemical weapons using the stolen materials as constituents.

Consequences are used as one of the key factors in determining the criticality of the asset and the degree of security countermeasures required. During the facility characterization step, consequences are used to screen low value assets from further consideration. For example, terrorists are assumed to be uninterested in low consequence assets (those that do not meet their criteria for valuable impacts).

## 2.4 ASSET ATTRACTIVENESS

Not all assets are of equal value to adversaries. A basic assumption of the SVA process is that this perception of value from an adversary's perspective is a factor that influences the likelihood of a security event. Asset attractiveness is an estimate of the real or perceived value of a target to an adversary based on such factors as shown in Figure 2.3.

During the SVA, the attractiveness of each asset should be evaluated based on the adversary's intentions or anticipated level of interest in the target. Security strategies can be developed around the estimated targets and potential threats. This factor, along with consequences, are used to screen facilities from more specific scenario analysis and from further specific countermeasures considerations during the first screening of the methodology.

Figure 2.3—Asset Attractiveness Factors

<b>Type of effect:</b>
• Potential for causing maximum casualties
• Potential for causing maximum damage and economic loss to the facility and company
• Potential for causing maximum damage and economic loss to the geographic region
• Potential for causing maximum damage and economic loss to the national infrastructure
<b>Type of target:</b>
• Usefulness of the process material as a weapon or to cause collateral damage
• Proximity to a national asset or landmark
• Difficulty of attack including ease of access and degree of existing security measures (soft target)
• High company reputation and brand exposure
• Iconic or symbolic target
• Chemical or biological weapons precursor chemical
• Recognition of the target



## 2.5 THREAT

Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Sources of threats may be categorized as:

- Terrorists (international or domestic);
- Activists, pressure groups, single-issue zealots;
- Disgruntled employees or contractors;
- Criminals (e.g., white collar, cyber hacker, organized, opportunists).

Threat information is important reference data to allow the Owner/Operator to understand the adversaries interested in the assets of the facility, their operating history, their methods and capabilities, their possible plans, and why they are motivated. This information should then be used to develop a design basis threat or threats.

Adversaries may be categorized as occurring from three general types:

- Insider threats
- External threats
- Insiders working as colluders with external threats

Each applicable adversary type should be evaluated against each asset as appropriate to understand vulnerabilities.

## 2.6 VULNERABILITY

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and subsequent destruction or theft of an asset. Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical security, or operational security practices. In a SVA, vulnerabilities are evaluated either by broadly considering the threat and hazards of the assets they could attack or affect, or analyzed by considering multiple potential specific sequences of events (a scenario-based approach). For this SVA methodology, each critical asset is analyzed from at least an asset-based approach at first by considering consequences and attractiveness. If it is a specific high value target, then it is recommended to analyze the asset further using scenarios.

## 2.7 SVA APPROACH

The general approach is to apply risk assessment resources and, ultimately, special security resources primarily where justified based on the SVA results. The SVA process involves consideration of each facility from both the general viewpoint and specific asset viewpoint. Consideration at the general level is useful for determination of overall impacts of loss, infrastructure and interdependencies at the facility level, and outer perimeter analysis including access control and general physical security. For example, all facilities will maintain a minimum level of security with general countermeasures such as the plant access control strategy and administrative controls. Certain assets will justify a more specific level of security, such as additional surveillance or barriers, based on their value and expected level of interest to adversaries. The benefit of evaluating specific assets is that individual risks can be evaluated and specific countermeasures applied where justified in addition to more general countermeasures.

This SVA methodology uses this philosophy in several ways. The method is intended to be comprehensive and systematic in order to be thorough. First, it begins with the SVA team gaining an understanding of the entire facility, the assets that comprise the facility, the critical functions of the facility, and the hazards and impacts if these assets or critical functions are compromised. This results in an understanding of which assets and functions are 'critical' to the business operation. This is illustrated in Figure 2.4.

Criticality is defined both in terms of the potential impact to the workers, community, the environment and the company, as well as to the business importance of the asset. For example, a storage tank of a hazardous material may not be the most critical part of the operation of a process, but if attacked, it has the greatest combined impact so it may be given a high priority for further analysis and special security countermeasures.

Based on this first level of screening from all assets to critical assets, a critical asset list is produced. Next, the critical assets are reviewed in light of the threats. Adversaries may have different objectives, so the critical asset list is reviewed from each adversary's perspective and an asset attractiveness ranking is given. This factor is a quick measure of whether the adversary would value damaging, compromising, or stealing the asset, which serves as an indicator of the likelihood that an adversary would want to attack this asset and why.

If an asset is both critical (based on value and consequences) and attractive, then it is considered a "target" for purposes of the SVA. A target may optionally receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities.

As shown in Figure 2.4, all assets receive at least a general security review. This is accomplished by the SVA team's initial consideration of assets, along with a baseline security survey. General security considerations may be found in security references such as the countermeasures checklist provided in Appendix B.

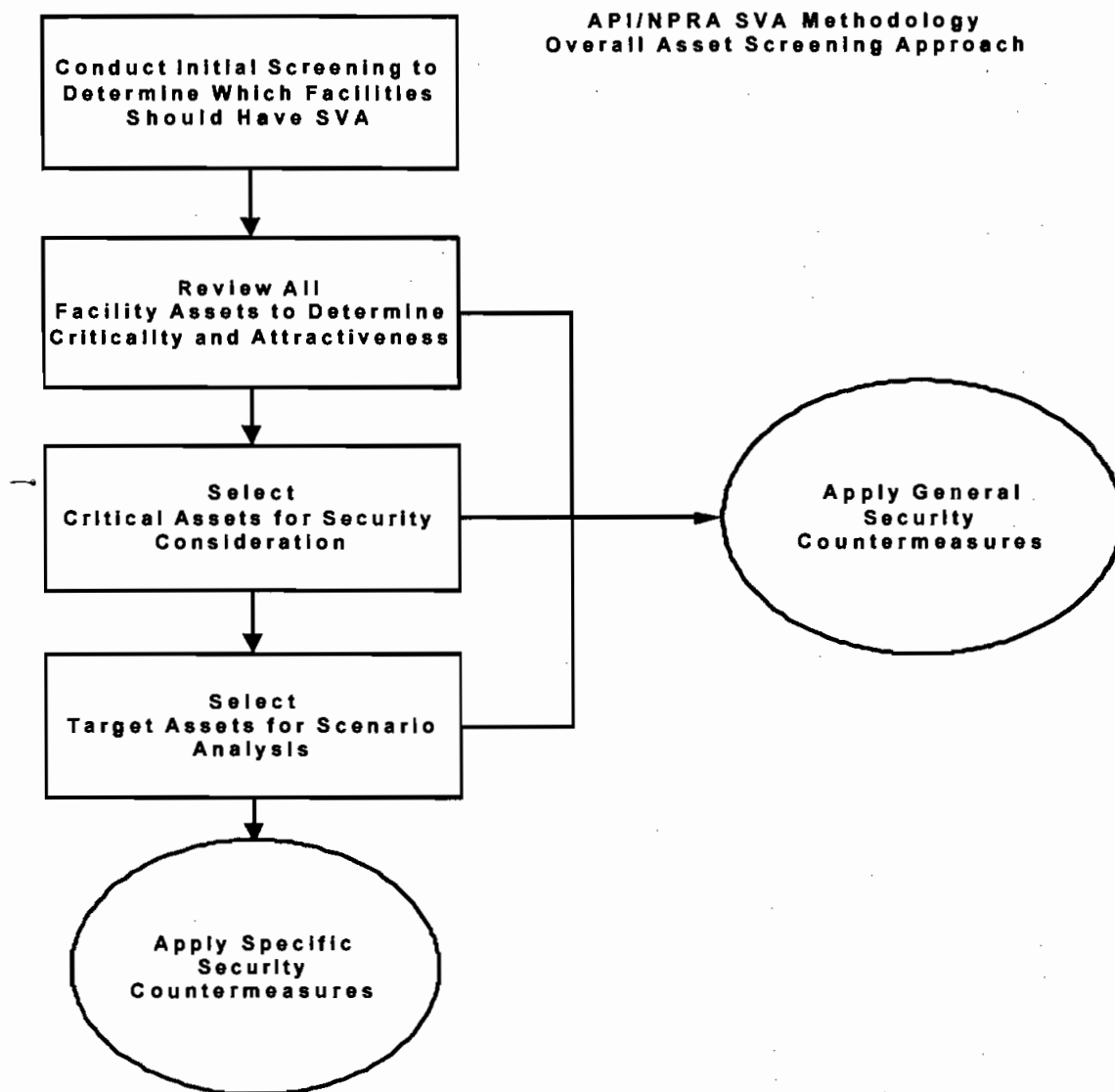


Figure 2.4—Overall Asset Screening Approach

All facilities should establish a security strategy. The general strategy is to protect against unauthorized access at the facility perimeter, and to control the access of authorized persons on the facility. Certain assets will be protected with added layers of protection, due to their attractiveness and consequences of loss. The specific security countermeasures provided to those assets would be to deter, detect, delay, and respond to credible threats against the assets to limit the risk to a certain level.

## 2.8 CHARACTERISTICS OF A SOUND SVA APPROACH

It is important to distinguish between a security risk management process and any given SVA methodology. Security risk management is the management framework that includes the SVA, development and implementation of a security plan, and the application of needed countermeasures to enhance security. SVA is the estimation of risk for the purposes of decision-making. SVA methodologies can be very powerful analytical tools to integrate data and information, and help understand the nature and locations of risks of a system. However, SVA methods alone should not be relied upon to establish risk, nor solely determine decisions about how risks should be addressed. SVA methods should be used as part of a process that involves knowledgeable and experienced personnel that critically review the input, assumptions, and results. The SVA team should integrate the SVA output with other factors, the impact of key assumptions, and the impact of uncertainties created by the absence of data or the variability in assessment inputs before arriving at decisions about risk and actions to reduce risk.

A variety of different approaches to SVA have been employed in the petroleum sector as well as other industries. The major differences among approaches are associated with:

- The relative “mix” of knowledge, data, or logic SVA methods;
- The complexity and detail of the SVA method; and
- The nature of the output (probabilistic versus relative measures of risk).

Ultimately, it is the responsibility of the owner/operator to choose the SVA method that best meets the needs of the company, the facilities and the agencies tasked with providing additional security in times of imminent danger. Therefore, it is in the best interest of the owner/operator to develop a thorough understanding of the various SVA methods in use and available, as well as the respective strengths and limitations of the different types of methods, before selecting a long-term strategy. A SVA should be:

- **Risk-based**—The approach should be to focus on the most significant security issues in a priority order based on risk. Risk can also be used to judge the adequacy of existing security measures.
- **Structured**—The underlying methodology must be structured to provide a thorough assessment. Some methodologies employ a more rigid structure than others. More flexible structures may be easier to use; however, they generally require more input from subject matter experts. However, all SVA methods identify and use logic to determine how the data considered contributes to risk in terms of affecting the likelihood and/or consequences of potential incidents.
- **Given adequate resources**—Appropriate personnel, time, and financial resources must be allocated to fit the detail level of the assessment.
- **Experience-based**—The frequency and severity of past security related events and the potential for future events should be considered. It is important to understand and account for any actions that have been made to prevent security related events. The SVA should consider the system-specific data and other knowledge about the system that has been acquired by field, operations, and engineering personnel as well as external expertise.
- **Predictive**—A SVA should be investigative in nature, seeking to identify recognized as well as previously unrecognized threats to the facility service and integrity. It should make use of previous security related events, but focus on the potential for future events, including the likelihood of scenarios that may never have happened before.
- **Based on the use of appropriate data**—Some SVA decisions are judgment calls. However, relevant data and particularly data about the system under review should affect the confidence level placed in the decisions.
- **Able to provide for and identify means of feedback**—SVA is an iterative process. Actual field drills, audits, and data collection efforts from both internal and external sources should be used to validate (or invalidate) assumptions made.

## 2.9 SVA STRENGTHS AND LIMITATIONS

Each of the SVA methods commonly used has its strengths and limitations. Some approaches are well suited to particular applications and decisions, but may not be as helpful in other situations. In selecting or applying SVA methods, there are a number of questions that should be considered. Some of the more significant ones are summarized below.

- Does the scope of the SVA method encompass and identify significant security related events and risks of the facility or along the system? If not, how can the risks that are not included in the SVA method be assessed and integrated in the future?
- Will all data be assessed, as it really exists along the system? Data should be location specific so that additive effects of the various risk variables can be determined. Can the assessment resolution be altered, e.g. station-by-station or mile-by-mile, dependent on the evaluation needs?
- What is the logical structure of variables that are evaluated to provide the qualitative and quantitative results of the SVA? Does this provide for straightforward data assimilation and assessment?
- Does the SVA method use numerical weights and other empirical factors to derive the risk measures and priorities? Are these weights based on the experience of the system, operator, industry, or external sources?
- Do the basic input variables of the SVA method require data that are available to the operator? Do operator data systems and industry data updating procedures provide sufficient support to apply the SVA method effectively? What is the process for updating the SVA data to reflect changes in the system, the infrastructure, and new security related data? How is the input data validated to ensure that the most accurate, up-to-date depiction of the system is reflected in the SVA?
- Does the SVA output provide adequate support for the justification of risk-based decisions? Are the SVA results and output documented adequately to support justification of the decisions made using this output?
- Does the SVA method allow for analysis of the effects of uncertainties in the data, structure, and parameter values on the method output and decisions being supported? What sensitivity or uncertainty analysis is supported by the SVA method?
- Does the SVA method focus exclusively on RMP-based “worst case” events or is it structured to determine “most probable worst case” events that may at times be less severe than postulated in an RMP or include additive effects of adjacent assets to yield consequences more severe than postulated in the RMP?

## 2.10 RECOMMENDED TIMES FOR CONDUCTING AND REVIEWING THE SVA

The SVA process or SVA methods can be applied at different stages of the overall security assessment and evaluation process. For example, it can be applied to help select, prioritize, and schedule the locations for security assessments. It can also be performed after the security assessment is completed to conduct a more comprehensive SVA that incorporates more accurate information about the facility or pipeline segment.

There are six occasions when the SVA may be required, as illustrated in Figure 2.5.

## 2.11 VALIDATION AND PRIORITIZATION OF RISKS

Independent of the process used to perform a SVA, the owner/operator must perform a quality control review of the output to ensure that the methodology has produced results consistent with the objectives of the assessment. This can be achieved through a review of the SVA data and results by a knowledgeable and experienced individual or, preferably, by a cross-functional team consisting of a mixture of personnel with skill sets and experience-based knowledge of the systems or segments being reviewed. This validation of the SVA method should be performed to ensure that the method has produced results that make sense to the operator. If the results are not consistent with the operator's understanding and expectations of system operation and risks, the operator should explore the reasons why and make appropriate adjustments to the method, assumptions, or data. Some additional criteria to evaluate the quality of a SVA are:

- Are the data and analyses handled competently and consistently throughout the system? (Can the logic be readily followed?)
- Is the assessment presented in an organized and useful manner?
- Are all assumptions identified and explained?
- Are major uncertainties identified, e.g., due to missing data?
- Do evidence, analysis, and argument adequately support conclusions and recommendations?

Once the SVA method and process has been validated, the operator has the necessary information to prioritize risks. To determine what risk mitigation actions to take, the operator considers which systems (or segments of systems) have the highest risks and then looks at the reasons the risks are higher for these assets. These risk factors are known as risk drivers since they drive the risk to a higher level for some assets than others do.

## 2.12 RISK SCREENING

Security issues exist at every facility managed by the petroleum and petrochemical industry, but the threat of intentional acts is likely to be different across the industry. This is captured by the factor known as 'asset attractiveness', whereby certain assets are considered to be more attractive to adversaries than others. Based on many reported threat assessments, intelligence reports, and actual events around the world, these factors can be used to evaluate target attractiveness.

It is likely that most facilities have no specific threat history for terrorism. As a result, the assumption must be made that potential malevolent acts are generally credible at each facility and this is then tempered by the site-specific factors. A screening process may contain the following factors:

1. Target attractiveness or target value;
2. Degree of threat;
3. Vulnerability;
4. Potential consequences (casualties, environmental, infrastructure and economic).

These are the same factors as are used for evaluating an individual asset risk, but the difference is that this is done at a generalized facility level for the risk screening instead of at a target asset level. Note that target attractiveness itself includes the factors of consequences and vulnerability. Target attractiveness is an aggregate of factors, which shows the complexity of the process of targeting. Consequences are listed again separately since they have such importance in targeting.

Consequence and target attractiveness are the dominant factors in determining terrorist risk. This is particularly true in the target-rich environment of the United States, where the rare nature of any particular terrorist act vs. the potential number of targets poses a major risk dilemma. Priority should first be given to the consequence ranking, but then consideration should be given to the attractiveness ranking when making assessments. In this way resources can be appropriately applied to assets where they are most likely to be important. This philosophy may be adopted by a company at an enterprise level to help determine both the need to conduct detailed (vs. simpler checklist analyses or audits), and the priority order for the analysis.

Figure 2.5—Recommended Times for Conducting and Reviewing the SVA

1	An initial review of all relevant facilities and assets per a schedule set during the initial planning process
2	When an existing process or operation is proposed to be substantially changed and prior to implementation (revision or rework)
3	When a new process or operation is proposed and prior to implementation (revision or rework)
4	When the threat substantially changes, at the discretion of the manager of the facility (revision or rework)
5	After a significant security incident, at the discretion of the manager of the facility (revision or rework)
6	Periodically to revalidate the SVA (revision or rework)

## Chapter 3 Conducting the Security Vulnerability Assessment Methodology

### 3.1 OVERVIEW OF THE SVA METHODOLOGY

The SVA process is a risk-based and performance-based methodology. The user can choose different means of accomplishing the general SVA method so long as the end result meets the same performance criteria. The overall 5-step approach of the SVA methodology is described as follows:

#### Step 1: Asset Characterization

The asset characterization includes analyzing information that describes the technical details of facility assets as required to support the analysis, identifying the potential critical assets, identifying the hazards and consequences of concern for the facility and its surroundings and supporting infrastructure, and identifying existing layers of protection.

#### Step 2: Threat Assessment

The consideration of possible threats should include internal threats, external threats, and internally assisted threats (i.e., collusion between insiders and outside agents). The selection of the threats should include reasonable local, regional, or national intelligence information, where available. This step includes determining the target attractiveness of each asset from each adversary's perspective.

**Step 3: Vulnerability Analysis**

The vulnerability analysis includes the relative pairing of each target asset and threat to identify potential vulnerabilities related to process security events. This involves the identification of existing countermeasures and their level of effectiveness in reducing those vulnerabilities.

The degree of vulnerability of each valued asset and threat pairing is evaluated by the formulation of security-related scenarios or by an asset protection basis. If certain criteria are met, such as higher consequence and attractiveness ranking values, then it may be useful to apply a scenario-based approach to conduct the Vulnerability Analysis. It includes the assignment of risk rankings to the security-related scenarios developed. If the asset-based approach is used, the determination of the asset's consequences and attractiveness may be enough to assign a target ranking value and protect via a standard protection set for that target level. In this case, scenarios may not be developed further than the general thought that an adversary is interested in damaging or stealing an asset.

**Step 4: Risk Assessment**

The risk assessment determines the relative degree of risk to the facility in terms of the expected effect on each critical asset as a function of consequence and probability of occurrence. Using the assets identified during Step 1 (Asset Characterization), the risks are prioritized based on the likelihood of a successful attack. Likelihood is determined by the team after considering the attractiveness of the targeted assets assessed under Step 2, the degree of threats assessed under Step 2, and the degree of vulnerability identified under Step 3.

**Step 5: Countermeasures Analysis**

Based on the vulnerabilities identified and the risk that the layers of security are breached, appropriate enhancements to the security countermeasures may be recommended. Countermeasure options will be identified to further reduce vulnerability at the facility. These include improved countermeasures that follow the process security doctrines of deter, detect, delay, respond, mitigate and possibly prevent. Some of the factors to be considered are:

- Reduced probability of successful attack
- Degree of risk reduction by the options
- Reliability and maintainability of the options
- Capabilities and effectiveness of mitigation options
- Costs of mitigation options
- Feasibility of the options

The countermeasure options should be re-ranked to evaluate effectiveness, and prioritized to assist management decision making for implementing security program enhancements. The recommendations should be included in a SVA report that can be used to communicate the results of the SVA to management for appropriate action.

Once the SVA is completed, there is a need to follow-up on the recommended enhancements to the security countermeasures so they are properly reviewed, tracked, and managed until they are resolved. Resolution may include adoption of the SVA team's recommendations, substitution of other improvements that achieve the same level of risk abatement, or rejection. Rejection of a SVA recommendation and related acceptance of residual risk should be based on valid reasons that are well documented.

This SVA process is summarized in Figure 3.1 and illustrated further in the flowcharts that follow in Figures 3.1a through 3.1c. Section 3.2 of this chapter describes the preparation activities, such as data gathering and forming the SVA team. Sections 3.3 through 3.8 provide details for each step in the SVA methodology. These steps and associated tasks are also summarized in Figure 3.5.

Figure 3.1—Security Vulnerability Assessment Methodology Steps

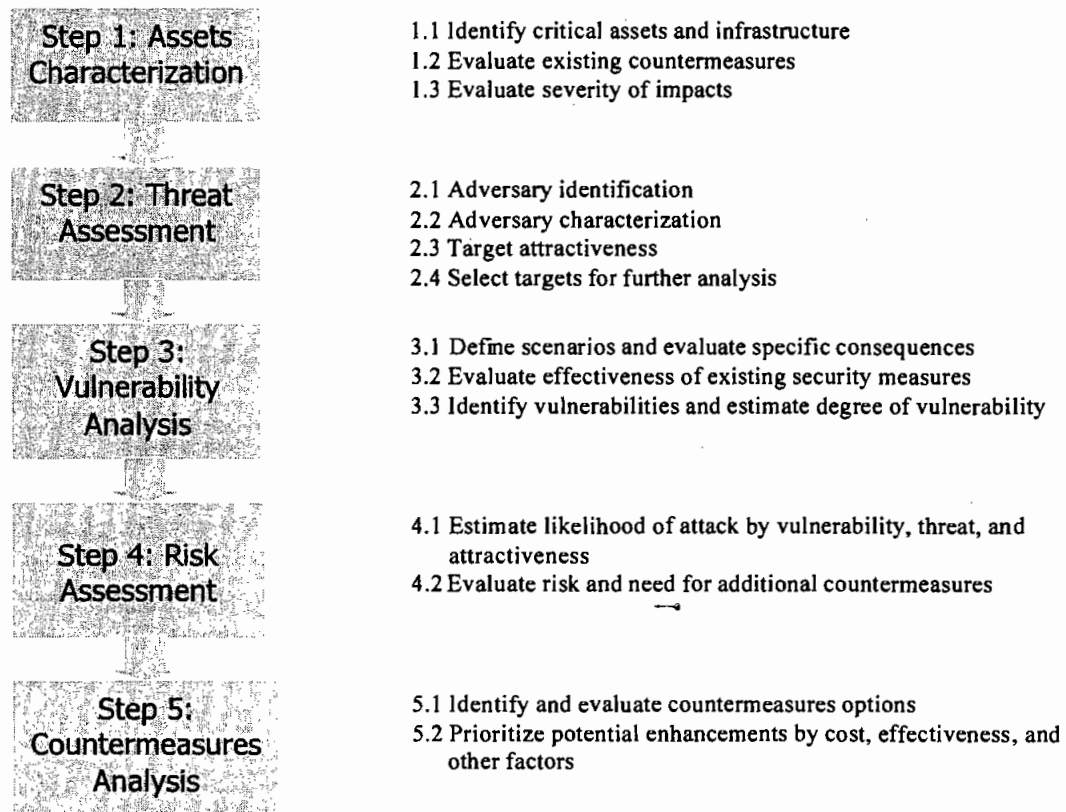


Figure 3.1a—Security Vulnerability Assessment Methodology—Step 1

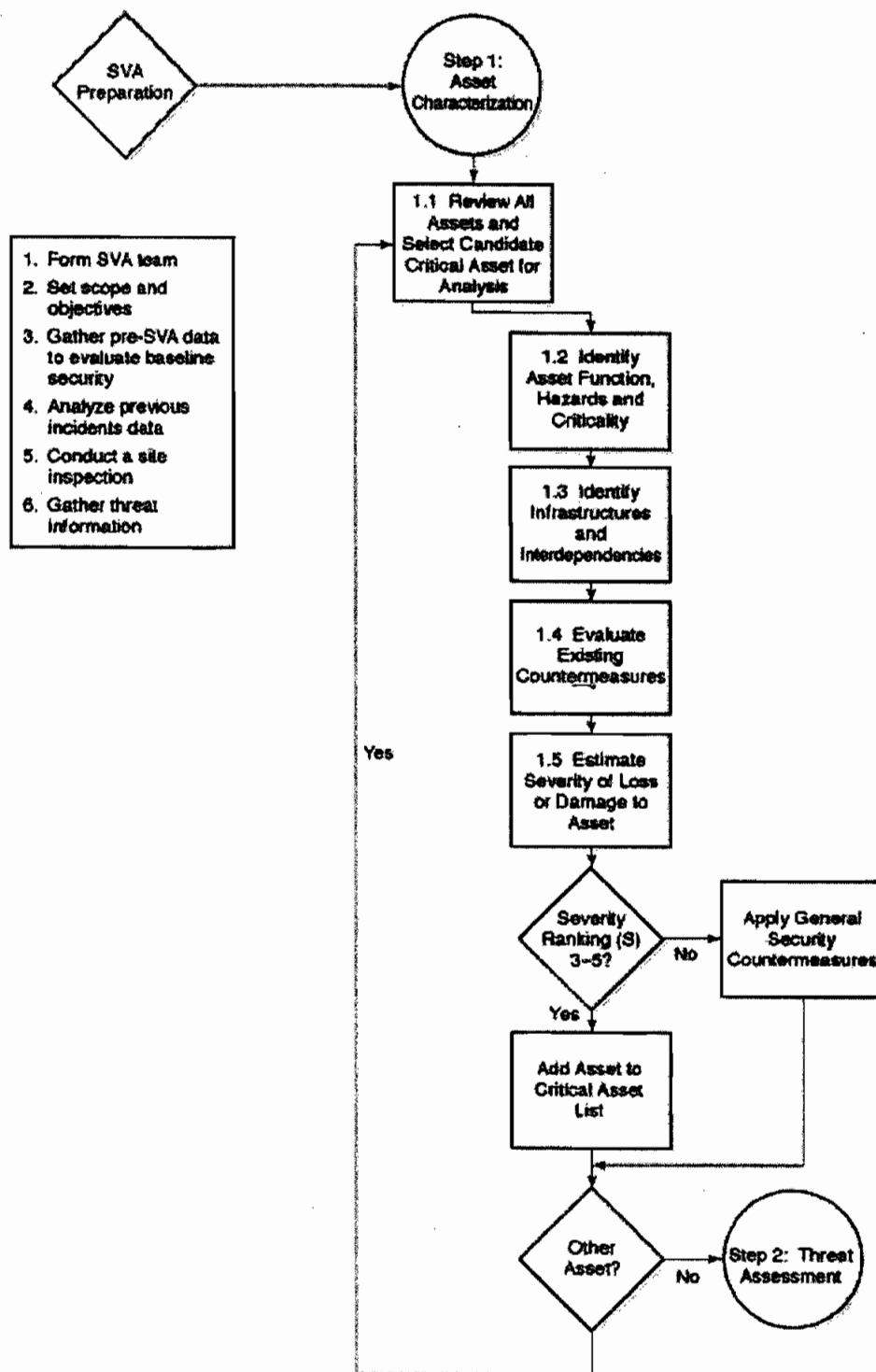




Figure 3.1b—Security Vulnerability Assessment Methodology—Step 2

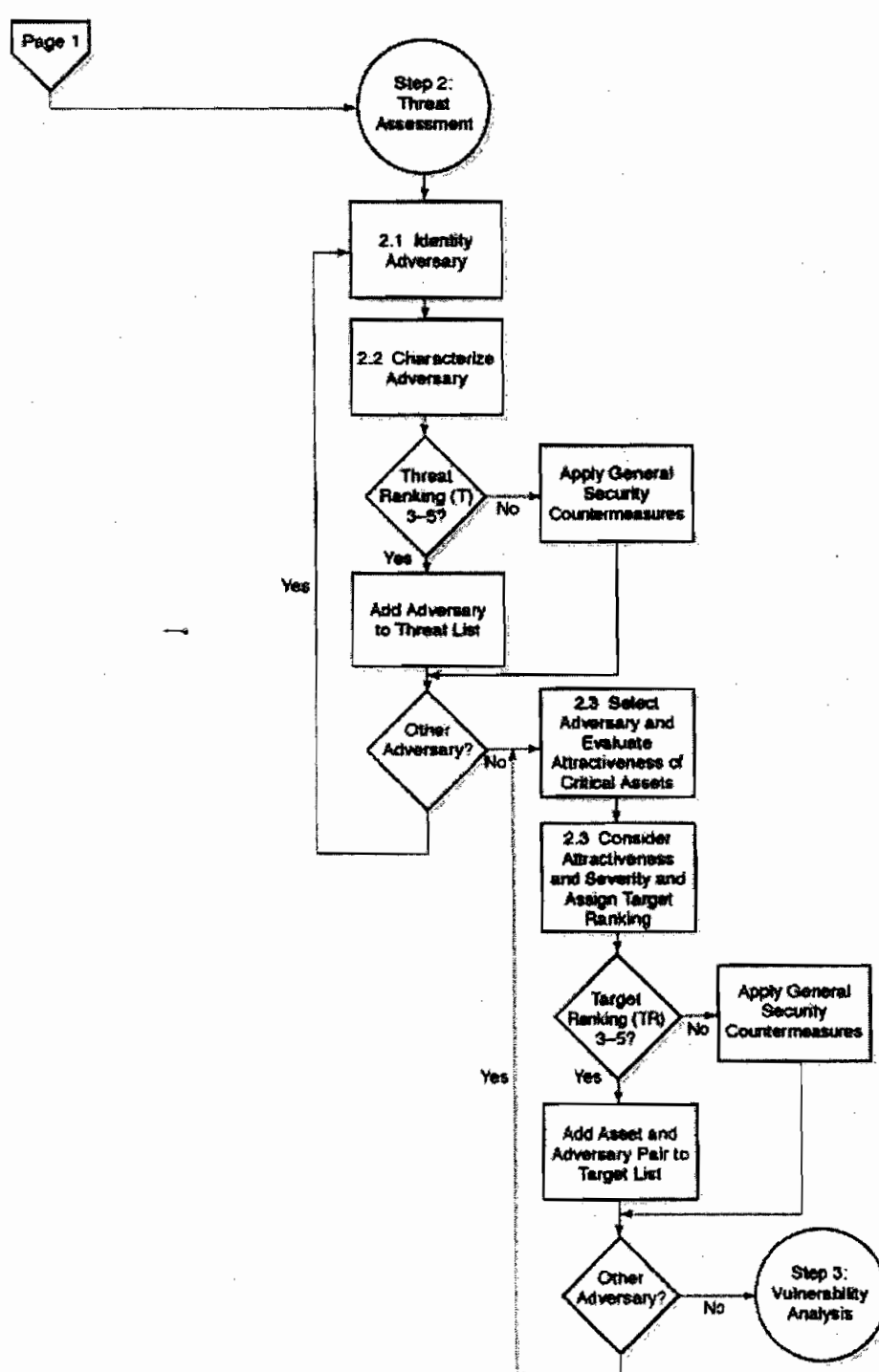
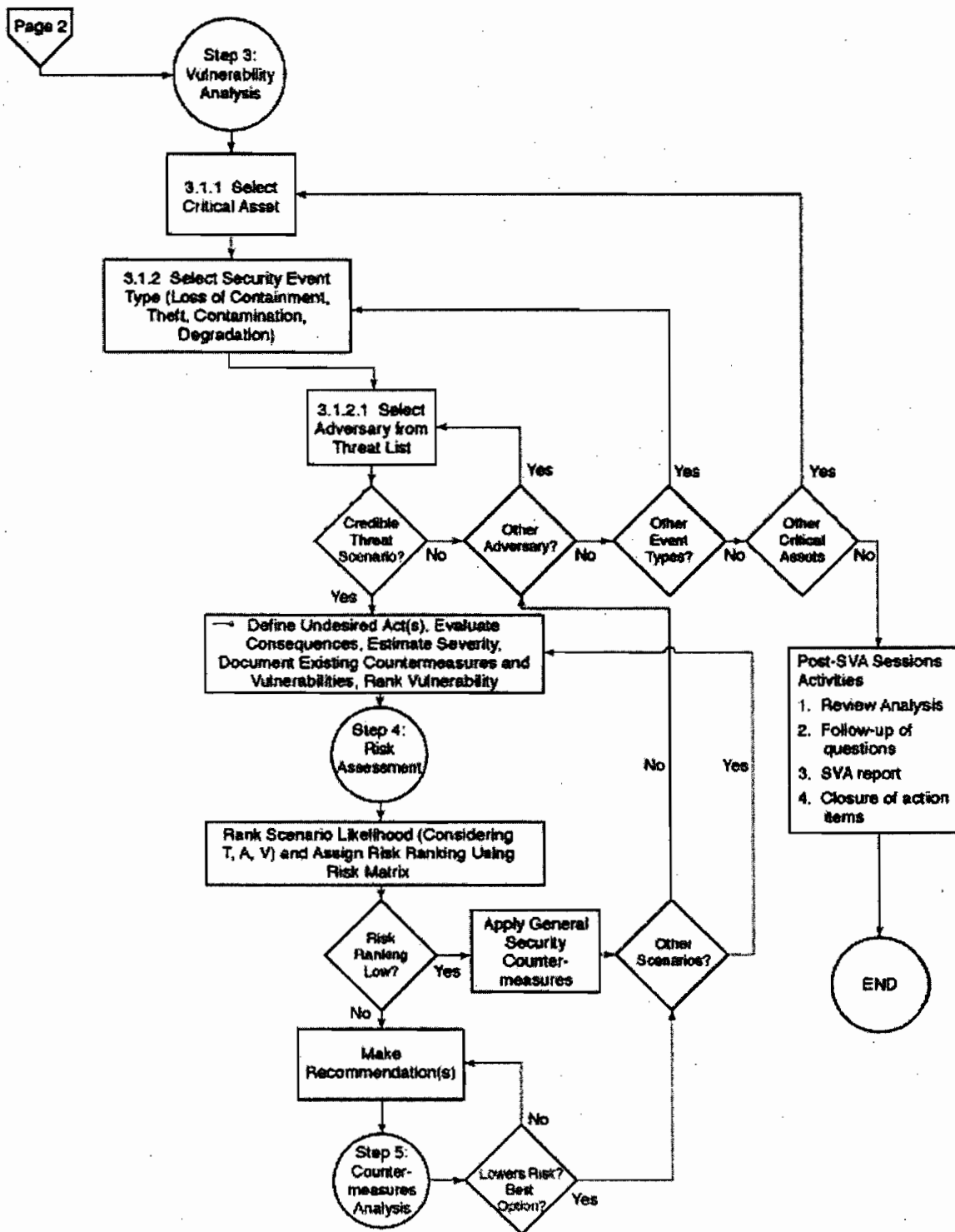


Figure 3.1c—Security Vulnerability Assessment Methodology—Steps 3 – 5



## 3.2 SVA PREPARATION

### 3.2.1 Planning for Conducting a SVA

Prior to conducting the SVA team-based sessions, there are a number of activities that must be done to ensure an efficient and accurate analysis. There are many factors in successfully completing a SVA including the following:

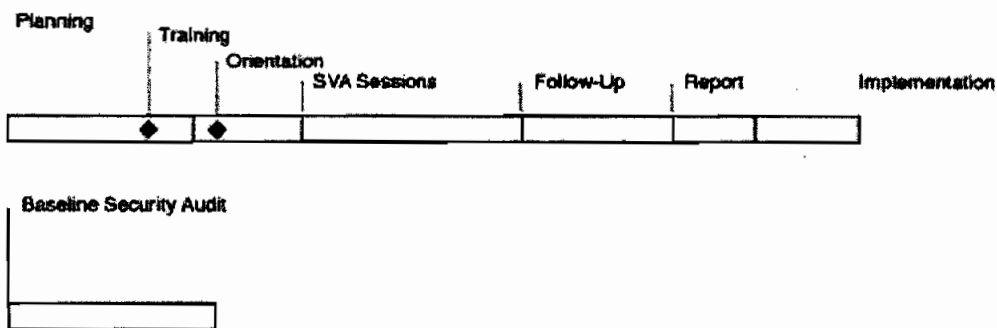
- the activity should be planned well in advance;
- have the full support and authorization by management to proceed;
- the data should be verified and complete;
- the objectives and scope should be concise;
- the team should be knowledgeable of and experienced at the process they are reviewing; and,
- the team leader should be knowledgeable and experienced in the SVA process methodology.

All of the above items are controllable during the planning stage prior to conducting the SVA sessions. Most important for these activities is the determination of SVA specific objectives and scope, and the selection and preparation of the SVA Team.

Prerequisites to conducting the SVA include gathering study data, gathering and analyzing threat information, forming a team, training the team on the method to be used, conducting a baseline security survey, and planning the means of documenting the process.

The typical timeline for conducting a SVA is shown in Figure 3.2.

Figure 3.2—SVA Methodology Timeline



### 3.2.2 SVA Team

The SVA approach includes the use of a representative group of company experts plus outside experts if needed to identify potential security related events or conditions, the consequences of these events, and the risk reduction activities for the operator's system. These experts draw on the years of experience, practical knowledge, and observations from knowledgeable field operations and maintenance personnel in understanding where the security risks may reside and what can be done to mitigate or ameliorate them.

Such a company group typically consists of representation from: company security, risk management, operations, engineering, safety, environmental, regulatory compliance, logistics/distribution, IT and other team members as required. This group of experts should focus on the vulnerabilities that would enhance the effectiveness of the facility security plan. The primary goal of this group is to capture and build into the SVA method the experience of this diverse group of individual experts so that the SVA process will capture and incorporate information that may not be available in typical operator databases.

If the scope of the SVA includes terrorism and attacks on a process handling flammable or toxic substances, the SVA should be conducted by a team with skills in both the security and process safety areas. This is because the team must evaluate traditional facility security as well as process-safety related vulnerabilities and countermeasures. The final security strategy for protection of the process assets from these events is a combination of security and process safety strategies.

It is expected that a full time 'core' team is primarily responsible, and that they are led by a Team Leader. Other part-time team members, interviewees and guests are used as required for efficiency and completeness. At a minimum, SVA

teams should possess the knowledge and/or skills listed in Figure 3.3. Other skills that should be considered and included, as appropriate, are included as optional or part-time team membership or as guests and persons interviewed.

The SVA Core Team is typically made up of three to five persons, but this is dependent on the number and type of issues to be evaluated and the expertise required to make those judgments. The Team Leader should be knowledgeable and experienced in the SVA approach.

### 3.2.3 SVA Objectives and Scope

The SVA Team leader should develop an objectives and scope statement for the SVA. This helps to focus the SVA and ensure completeness. An example SVA objectives statement is shown in Figure 3.4.

A work plan should then be developed to conduct the SVA with a goal of achieving the objectives. The work plan needs to include the scope of the effort, which includes which physical or cyber facilities and issues will be addressed.

Given the current focus on the need to evaluate terrorist threats, the key concerns are the intentional (malevolent) misuse of petroleum and hazardous to cause catastrophic consequences. Given this focus, the key events and consequences of interest include the four listed in Figure 3.5. Other events may be included in the scope as determined by the SVA Team, but it is recommended that these four primary security events be addressed first since these are the events that make the petroleum and petrochemical industry unique from other industries.

Figure 3.3—SVA Team Members

**The SVA Core Team** members should have the following skill sets and experience:

- Team leader—knowledge of and experience with the SVA methodology;
- Security representative—knowledge of facility security procedures, methods and systems;
- Safety representative—knowledge of potential process hazards, process safety procedures, methods, and systems of the facility;
- Facility representative—knowledge of the design of the facility under study including asset value, function, criticality, and facility procedures;
- Operations representative—knowledge of the facility process and equipment operation;
- Information systems/Automation representative (for cyber security assessment)—knowledge of information systems technologies and cyber security provisions; knowledge of process control systems.

**The SVA Optional/Part-time Team** members may include the following skill sets and experience:

- Security specialist—knowledge of threat assessment, terrorism, weapons, targeting and insurgency/guerilla warfare, or specialized knowledge of detection technologies or other countermeasures available;
- Cyber security specialist—knowledge of cyber security practices and technologies;
- Subject matter experts on various process or operations details such as process technologies, rotating equipment, distributed control systems, electrical systems, access control systems, etc.;
- Process specialist—knowledge of the process design and operations
- Management—knowledge of business management practices, goals, budgets, plans, and other management systems.

Figure 3.4—Sample Objectives Statement<sup>8</sup>

To conduct an analysis to identify security hazards, threats, and vulnerabilities facing a fixed facility handling hazardous materials, and to evaluate the countermeasures to provide for the protection of the public, workers, national interests, the environment, and the company.

<sup>7</sup>Ibid, AIChE.

<sup>8</sup>Ibid, AIChE.

Figure 3.5—Security Events of Concern

Security Event Type	Candidate Critical Assets
Loss of Containment, Damage, or Injury	Loss of containment of process hydrocarbons or hazardous chemicals on the plant site from intentional damage of equipment or the malicious release of process materials, which may cause multiple casualties, severe damage, and public or environmental impact. Also included is injury to personnel and the public directly or indirectly
Theft	Hydrocarbon, chemical, or information theft or misuse with the intent to cause severe harm at the facility or offsite
Contamination	Contamination or spoilage of plant products or information to cause worker or public harm on or offsite
Degradation of Assets	Degradation of assets or infrastructure or the business function or value of the facility or the entire company through destructive acts of terrorism.

### 3.2.4 Data Gathering, Review, and Integration

The objective of this step is to provide a systematic methodology for Owner/Operators to obtain the data needed to manage the security of their facility. Most Owner/Operators will find that many of the data elements suggested here are already being collected. This section provides a systematic review of potentially useful data to support a security plan. However, it should be recognized that all of the data elements in this section are not necessarily applicable to all systems.

The types of data required depend on the types of risks and undesired acts that are anticipated. The operator should consider not only the risks and acts currently suspected in the system, but also consider whether the potential exists for other risks and acts not previously experienced in the system, e.g., bomb blast damage. This section includes lists of many types of data elements. The following discussion is separated into four subsections that address sources of data, identification of data, location of data, and data collection and review.

Appendix A includes a list of potentially useful data that may be needed to conduct a SVA. Appendix B is a checklist of countermeasures that may be used as a data collection form prior to conducting a SVA. Similarly, Appendix C is a checklist for infrastructure and interdependencies that can be used both before and after a SVA for ensuring completeness.

#### 3.2.4.1 Data Sources

The first step in gathering data is to identify the sources of data needed for facility security management. These sources can be divided into four different classes.

1. **Facility and Right of Way Records.** Facility and right of way records or experienced personnel are used to identify the location of the facilities. This information is essential for determining areas and other facilities that either may impact or be impacted by the facility being analyzed and for developing the plans for protecting the facility from security risks. This information is also used to develop the potential impact zones and the relationship of such impact zones to various potentially exposed areas surrounding the facility i.e., population centers, and industrial and government facilities.
2. **System Information.** This information identifies the specific function of the various parts of the process and their importance from a perspective of identifying the security risks and mitigations as well as understanding the alternatives to maintaining the ability of the system to continue operations when a security threat is identified. This information is also important from a perspective of determining those assets and resources available in-house in developing and completing a security plan. Information is also needed on those systems in place, which could support a security plan such as an integrity management program and IT security functions.
3. **Operation Records.** Operating data are used to identify the products transported and the operations as they may pertain to security issues to facilities and pipeline segments which may be impacted by security risks. This information is also needed to prioritize facilities and pipeline segments for security measures to protect the system, e.g., type of product, facility type and location, and volumes transported. Included in operation records data gathering is the need to obtain incident data to capture historical security events.
4. **Outside Support and Regulatory Issues.** This information is needed for each facility or pipeline segment to determine the level of outside support that may be needed and can be expected for the security measures to be employed at each facility or pipeline segment. Data are also needed to understand the expectation for security preparedness and coordination from the regulatory bodies at the government, state, and local levels. Data should also be developed on communication and other infrastructure issues as well as sources of information regarding security threats, e.g., ISACs (Information Sharing and Analysis Centers).

### 3.2.4.2 Identifying Data Needs

The type and quantity of data to be gathered will depend on the individual facility or pipeline system, the SVA methodology selected, and the decisions that are to be made. The data collection approach will follow the SVA path determined by the initial expert team assembled to identify the data needed for the first pass at SVA. The size of the facility or pipeline system to be evaluated and the resources available may prompt the SVA team to begin their work with an overview or screening assessment of the most critical issues that impact the facility or pipeline system with the intent of highlighting the highest risks. Therefore, the initial data collection effort will only include the limited information necessary to support this SVA. As the SVA process evolves, the scope of the data collection will be expanded to support more detailed assessment of perceived areas of vulnerability.

### 3.2.4.3 Locating Required Data

Operator data and information are available in different forms and format. They may not all be physically stored and updated at one location based on the current use or need for the information. The first step is to make a list of all data required for security vulnerability assessment and locate the data. The data and information sources may include:

- Facility plot plans, equipment layouts and area maps
- Process and Instrument Drawings (P&IDs)
- Pipeline alignment drawings
- Existing company standards and security best practices
- Product throughput and product parameters
- Emergency response procedures
- Company personnel interviews
- LEPC (Local Emergency Planning Commission) response plans
- Police agency response plans
- Historical security incident reviews
- Support infrastructure reviews

### 3.2.4.4 Data Collection and Review

Every effort should be made to collect good quality data. When data of suspect quality or consistency are encountered, such data should be flagged so that during the assessment process, appropriate confidence interval weightings can be developed to account for these concerns.

In the event that the SVA approach needs input data that are not readily available, the operator should flag the absence of information. The SVA team can then discuss the necessity and urgency of collecting the missing information.

### 3.2.5 Analyzing Previous Incidents Data

Any previous security incidents relevant to the security vulnerability assessment may provide valuable insights to potential vulnerabilities and trends. These events from the site and, as available, from other historical records and references, should be considered in the analysis. This may include crime statistics, case histories, or intelligence relevant to facility.

### 3.2.6 Conducting a Site Inspection

Prior to conducting the SVA sessions, it is necessary for the team to conduct a site inspection to visualize the facility and to gain valuable insights to the layout, lighting, neighboring area conditions, and other facts that may help understand the facility and identify vulnerabilities. The list of data requirements in Appendix A and the checklist in Appendix B may be referenced for this purpose.

### 3.2.7 Gathering Threat Information

The team should gather and analyze relevant company and industry or government-provided threat information, such as that available from the Energy ISAC, DHS, FBI, or other local law enforcement agency.

## 3.3 STEP 1: ASSETS CHARACTERIZATION

Characterization of the facility is a step whereby the facility assets and hazards are identified, and the potential consequences of damage or theft to those assets is analyzed. The focus is on processes which may contain petroleum or hazardous chemicals and key assets, with an emphasis on possible public impacts. The Asset Attractiveness, based on

these and other factors, is included in the facility characterization. These two factors (severity of the consequences and asset attractiveness) are used to screen the facility assets into those that require only general vs. those that require more specific security countermeasures.

The team produces a list of candidate critical assets that need to be considered in the analysis. Attachment 1—Step 1: Critical Assets/Criticality Form is helpful in developing and documenting the list of critical assets. The assets may be processes, operations, personnel, or any other asset as described in Chapter 3.

Figure 3.6 below summarizes the key steps and tasks required for Step 1.

### Step 1.1—Identify Critical Assets

The SVA Team should identify critical assets for the site being studied. The focus is on petroleum or chemical process assets, but any asset may be considered. For example, the process control system may be designated as critical, since protection of it from physical and cyber attack may be important to prevent a catastrophic release or other security event of concern. Figure 3.7 is an example list of specific assets that may be designated as critical at any given site. Assets include the full range of both material and non-material aspects that enable a facility to operate.

Figure 3.6—Description of Step 1 and Substeps

Step	Task
<b>Step 1: Assets Characterization</b>	
1.1 Identify critical assets	Identify critical assets of the facility including people, equipment, systems, chemicals, products, and information.
1.2 Identify critical functions	Identify the critical functions of the facility and determine which assets perform or support the critical functions.
1.3 Identify critical infrastructures and interdependencies	Identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset.
1.4 Evaluate existing countermeasures	Identify what protects and supports the critical functions and assets. Identify the relevant layers of existing security systems including physical, cyber, operational, administrative, and business continuity planning, and the process safety systems that protect each asset.
1.5 Evaluate impacts	Evaluate the hazards and consequences or impacts to the assets and the critical functions of the facility from the disruption, damage, or loss of each of the critical assets or functions.
1.6 Select targets for further analysis	Develop a target list of critical functions and assets for further study.

Figure 3.7—Example Candidate Critical Assets

Security Event Type	Candidate Critical Assets
Loss of Containment, Damage, or Injury	<ul style="list-style-type: none"> <li>• Process equipment handling petroleum and hazardous materials including processes, pipelines, storage tanks</li> <li>• Marine vessels and facilities, pipelines, other transportation systems</li> <li>• Employees, contractors, visitors in high concentrations</li> </ul>
Theft	<ul style="list-style-type: none"> <li>• Hydrocarbons or chemicals processed, stored, manufactured, or transported</li> <li>• Metering stations, process control and inventory management systems</li> <li>• Critical business information from telecommunications and information management systems including Internet accessible assets</li> </ul>
Contamination	<ul style="list-style-type: none"> <li>• Raw material, intermediates, catalysts, products, in processes, storage tanks, pipelines</li> <li>• Critical business or process data</li> </ul>
Degradation of Assets	<ul style="list-style-type: none"> <li>• Processes containing petroleum or hazardous chemicals</li> <li>• Business image and community reputation</li> <li>• Utilities (electric power, steam, water, natural gas, specialty gases)</li> <li>• Telecommunications Systems</li> <li>• Business systems</li> </ul>

The following information should be reviewed by the SVA Team as appropriate for determination of applicability as critical assets:

- Any applicable regulatory lists of highly hazardous chemicals, such as the Clean Air Act 112(r) list of flammable and toxic substances for the EPA Risk Management Program (RMP) 40 *CFR* Part 68 or the OSHA Process Safety Management (PSM) 29 *CFR* 1910.119 list of highly hazardous chemicals;
- Inhalation poisons or other chemicals that may be of interest to adversaries;
- Large and small scale chemical weapons precursors as based on the following lists:
  - Chemical Weapons Convention list;
  - FBI Community Outreach Program (FBI List) for Weapons of Mass Destruction materials and precursors;
  - The Australia Group list of chemical and biological weapons
- Material destined for the food, nutrition, cosmetic or pharmaceutical chains;
- Chemicals which are susceptible to reactive chemistry.

Owner/Operators may wish to consider other categories of chemicals that may cause losses or injuries that meet the objectives and scope of the analysis. These may include other flammables, critically important substances to the process, explosives, radioactive materials, or other chemicals of concern.

In addition, the following personnel, equipment and information may be determined to be critical:

- Process equipment
- Critical data
- Process control systems
- Personnel
- Critical infrastructure and support utilities

### Step 1.2—Identify Critical Functions

The SVA Team should identify the critical functions of the facility and determine which assets perform or support the critical functions. For example, the steam power plant of a refinery may be critical since it is the sole source of steam supply to the refinery.

### Step 1.3—Identify Critical Infrastructures and Interdependencies

The SVA team should identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset. For example, the electrical substation may be the sole electrical supply to the plant, or a supplier delivers raw material to the facility via a single pipeline. Appendix C, Interdependencies and Infrastructure Checklist, can be used to identify and analyze these issues. Note that some of these issues may be beyond the control of the owner/operator, but it is necessary to understand the dependencies and interdependencies of the facility, and the result of loss of these systems on the process.



### Step 1.4—Evaluate Existing Countermeasures

The SVA team identifies and documents the existing security and process safety layers of protection. This may include physical security, cyber security, administrative controls, and other safeguards. During this step the objective is to gather information on the types of strategies used, their design basis, and their completeness and general effectiveness. A pre-SVA survey is helpful to gather this information. The data will be made available to the SVA team for them to form their opinions on the adequacy of the existing security safeguards during Step 3: Vulnerability Analysis and Step 5: Countermeasures Analysis.

Appendix B—Countermeasures Survey Form can be used to gather information on the presence and status of existing safeguards or another form may be more suitable. Existing records and documentation on security and process safety systems, as well as on the critical assets themselves, can be referenced rather than repeated in another form of documentation.

The objective of the physical security portion of the survey is to identify measures that protect the entire facility and/or each critical asset of the facility, and to determine the effectiveness of the protection. Appendix B contains checklists that may be used to conduct the physical security portion of the survey.

Note that the infrastructure interdependencies portion of the survey will identify infrastructures that support the facility and/or its critical assets (e.g., electric power, water, and telecommunications). A physical security review of these vital infrastructures should also be conducted.

### Step 1.5—Evaluate Impacts

The Impacts Analysis step includes both the determination of the hazards of the asset being compromised as well as the specific consequences of a loss. The SVA team should consider relevant chemical use and hazard information, as well as information about the facility. The intent is to develop a list of target assets that require further analysis partly based on the degree of hazard and consequences. Particular consideration should be given to the hazards of fire, explosion, toxic release, radioactive exposure, and environmental contamination.

The consequences are analyzed to understand their possible significance. The Appendix A—Attachment 1—Step 1: Critical Assets/Criticality Form is useful to document the general consequences for each asset. The consequences may be generally described but consideration should be given to those listed in Figure 3.8.

Figure 3.8—Possible Consequences of Security Events

Public fatalities or injuries
Site personnel fatalities or injuries
Large-scale disruption to the national economy, public or private operations
Large-scale disruption to company operations
Large-scale environmental damage
Large-scale financial loss
Loss of critical data
Loss of reputation or business viability

The consequence analysis is done in a general manner. If the security event involves a toxic or flammable release to the atmosphere, the EPA RMP offsite consequence analysis guidance can be used as a starting point. If it is credible to involve more than the largest single vessel containing the hazardous material in a single incident, the security event may be larger than the typical EPA RMP worst-case analysis.

A risk ranking scale can be used to rank the degree of severity. Figure 3.9 illustrates a set of consequence definitions based on four categories of events—A. Fatalities and injuries; B. Environmental impacts; C. Property damage; and D. Business interruption.

Figure 3.9—Example Definitions of Consequences of the Event

DESCRIPTION	RANKING
A. Possible for any offsite fatalities from large-scale toxic or flammable release; possible for multiple onsite fatalities B. Major environmental impact onsite and/or offsite (e.g., large-scale toxic contamination of public waterway) C. Over \$X property damage D. Very long term (> X years) business interruption/expense; Large-scale disruption to the national economy, public or private operations; Loss of critical data; Loss of reputation or business viability	<b>S5 – Very High</b>
A. Possible for onsite fatalities; possible offsite injuries B. Very large environmental impact onsite and/or large offsite impact C. Over \$X – \$Y property damage D. Long term (X months – Y years) business interruption/expense	<b>S4 – High</b>
A. No fatalities or injuries anticipated offsite; possible widespread onsite serious injuries B. Environmental impact onsite and/or minor offsite impact C. Over \$X – \$Y property damage D. Medium term (X months – Y months) business interruption/expense	<b>S3 – Medium</b>
A. Onsite injuries that are not widespread but only in the vicinity of the incident location; No fatalities or injuries anticipated offsite B. Minor environmental impacts to immediate incident site area only C. \$X – \$Y loss property damage D. Short term (up to X months) business interruption/expense	<b>S2 – Low</b>
A. Possible minor injury onsite; No fatalities or injuries anticipated offsite B. No environmental impacts C. Up to \$X Property Damage D. Very short term (up to X weeks) business interruption/expense	<b>S1 – Very Low</b>

The consequences of a security event at a facility are generally expressed in terms of the degree of acute health effects (e.g., fatality, injury), property damage, environmental effects, etc. This definition of consequences is the same as that used for accidental releases, and is appropriate for security-related events. The key difference is that they may involve effects that are more severe than expected with accidental risk. This difference has been considered in the steps of the SVA.

The SVA Team should evaluate the potential consequences of an attack using the judgment of the SVA team. If scenarios are done, the specific consequences may be described in scenario worksheets.

Team members skilled and knowledgeable in the process technology should review any off-site consequence analysis data previously developed for safety analysis purposes or prepared for adversarial attack analysis. The consequence analysis data may include a wide range of release scenarios if appropriate.

Proximity to off-site population is a key factor since it is both a major influence on the person(s) selecting a target, and on the person(s) seeking to defend that target. In terms of attractiveness to a terrorist, if the target could expose a large number of persons, this type of target is likely to be a high-value, high-payoff target.

#### Step 1.6—Select Targets for Further Analysis

For each asset identified, the criticality of each asset must be understood. This is a function of the value of the asset, the hazards of the asset, and the consequences if the asset was damaged, stolen, or misused. For hazardous chemicals, consideration may include toxic exposure to workers or the community, or potential for the misuse of the chemical to produce a weapon or the physical properties of the chemical to contaminate a public resource.

The SVA Team develops a Target Asset List which is a list of the assets associated with the site being studied that are more likely to be attractive targets, based on the complete list of assets and the identified consequences and targeting issues identified in the previous steps. During Step 3: Vulnerability Analysis, the Target Asset List will be generally paired with specific threats and evaluated against the potential types of attack that could occur.

The SVA methodology uses ranking systems that are based on a scale of 1 – 5 where 1 is the lowest value and 5 is the highest value. Based on the consequence ranking and criticality of the asset, the asset is tentatively designated a candidate critical target asset. The attractiveness of the asset will later be used for further screening of important assets.

### 3.4 STEP 2: THREAT ASSESSMENT

The threat assessment step involves the substeps shown in Figure 3.10.

#### Step 2.1—Adversary Identification

The next step is to identify specific classes of adversaries that may perpetrate the security-related events. The adversary characterization sub-step involves developing as complete an understanding as is possible of the adversary's history, capabilities and intent. A threat matrix is developed to generally pair the assets with each adversary class as shown in Attachment 1—Step 2: Threat Assessment Form.

Figure 3.10—Description of Step 2 and Substeps

Step	Task
<b>Step 2: Threat Assessment</b>	
2.1 Adversary identification	Evaluate threat information and identify threat categories and potential adversaries. Identify general threat categories. Consider threats posed by insiders, external agents (outsiders), and collusion between insiders and outsiders.
2.2 Adversary characterization	Evaluate each adversary and provide an overall threat assessment/ ranking for each adversary using known or available information. Consider such factors as the general nature/history of threat; specific threat experience/history to the facility/operation; known capabilities/methods/weapons; potential actions, intent/ motivation of adversary.
2.3 Analyze target attractiveness	Conduct an evaluation of target (from assets identified in Step 1) attractiveness from the adversary perspective.

Depending on the threat, the analyst can determine the types of potential attacks and, if specific information is available (intelligence) on potential targets and the likelihood of an attack, specific countermeasures may be taken. Information may be too vague to be useful, but SVA Teams should seek available information from Federal, State, and Local law enforcement officials in analyzing threats. Absent specific threat information, the SVA can still be applied based on assuming general capabilities and characteristics of typical hypothetical adversaries.

Threat assessment is an important part of a security management system, especially in light of the emergence of international terrorism in the United States. There is a need for understanding the threats facing the industry and any given facility or operation to properly respond to those threats. This section describes a threat assessment approach as part of the security management process. Later in Section 3.0 the use of the threat assessment in the SVA process will be more fully explained.

A threat assessment is used to evaluate the likelihood of adversary activity against a given asset or group of assets. It is a decision support tool that helps to establish and prioritize security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability, intention, and impact of an attack.

Threat assessment is a process that must be systematically done and kept current to be useful. The determination of these threats posed by different adversaries leads to the recognition of vulnerabilities and to the evaluation of required countermeasures to manage the threats. Without a design basis threat or situation specific threat in mind, a company cannot effectively develop a cost-effective security management system.

In characterizing the threat to a facility or a particular asset for a facility, a company should examine the historical record of security events and obtains available general and location-specific threat information from government organizations and other sources. It should then evaluate these threats in terms of company assets that represent likely targets.

Some threats are assumed continuous, whereas others are assumed to be variable. As such, this guidance follows the Department of Homeland Security's Homeland Security Advisory System (HSAS) and the U.S.C.G. Maritime Security (MARSEC) security levels for management of varying threat levels to the industry. The threat assessment determines the estimated general threat level, which varies as situations develop. Depending on the threat level, different security measures over baseline measures will likely be necessary.

While threat assessments are key decision support tools, it should be recognized that, even if updated often, threat assessments might not adequately capture emerging threats posed by some adversary groups. No matter how much we know about potential threats, we will never know that we have identified every threat or that we have complete information even about the threats of which we are aware. Consequently, a threat assessment must be accompanied by a vulnerability assessment to provide better assurance of preparedness for a terrorist or other adversary attack.

Intelligence and law enforcement agencies assess the foreign and domestic terrorist threats to the United States. The U.S. intelligence community—which includes the Central Intelligence Agency, the Defense Intelligence Agency, and the State Department's Bureau of Intelligence and Research, among others—monitors the foreign-origin terrorist threat to the United States. The FBI gathers information and assesses the threat posed by domestic sources of terrorism.

Threat information gathered by both the intelligence and law enforcement communities can be used to develop a company-specific threat assessment. A company attempts to identify threats in order to decide how to manage risk in a cost-effective manner. All companies are exposed to a multitude of threats, including terrorism or other forms of threat.

A threat assessment can take different forms, but the key components are:

1. Identification of known and potential adversaries;
2. Recognition and analysis of their intentions, motivation, operating history, methods, weapons, strengths, weaknesses, and intelligence capabilities;
3. Assessment of the threat posed by the adversary factors mentioned above against each asset, and the assignment of an overall criticality ranking for each adversary.

Threats need to be considered from both insiders and outsiders, or a combination of those adversaries working in collusion. Insiders are defined as those individuals who normally have authorized access to the asset. They pose a particularly difficult threat, due to the possibility for deceit, deception, training, knowledge of the facilities, and unsupervised access to critical information and assets.

The threat categories to be considered are those that include intent and capability of causing major catastrophic harm to the facilities and to the public or environment. Typical adversaries that may be included in a SVA are: international terrorists, domestic terrorists (including disgruntled individuals/'lone wolf' sympathizers), disgruntled employees, or extreme activists.

All companies are encouraged to discuss threats with local and Federal law enforcement officials, and to maintain networking with fellow industrial groups to improve the quality of applicable threat information.

The threat assessment is not necessarily based on perfect information. In fact, for most facilities, the best available information is vague or nonspecific to the facility. A particularly frustrating part of the analysis can be the absence of site-specific information on threats. A suggested approach is to make an assumption that international terrorism is possible at every facility that has adequate attractiveness to that threat. Site-specific information adjusts the generic average rankings accordingly.

To be effective, threat assessment must be considered a dynamic process, whereby the threats are continuously evaluated for change. During any given SVA exercise, the threat assessment is referred to for guidance on general or specific threats facing the assets. At that time the company's threat assessment should be referred to and possibly updated as required given additional information and analysis of vulnerabilities.

Figure 3.11 includes a five level ranking system for defining threats against an asset.

### **Step 2.2—Adversary Characterization**

Insiders, outsiders or a combination of the two may perpetrate an attack. Insiders are personnel that have routine, unescorted access within the facility. Outsiders do not. Collusion between the two may be the result of monetary gain (criminal insider/terrorist outsider), ideological sympathy, or coercion.

The adversary characterization will assist in evaluating the attack issues associated with insider, outsider, and colluding adversary threats. The SVA team should consider each type of adversary identified as credible, and generally define their level of capabilities, motivation, and likelihood of threat.

### **Step 2.3—Analyze Target Attractiveness**

The team assigns the target attractiveness ranking. To facilitate this use Attachment I—Threat Assessment: Target Attractiveness Form can be used.

The attractiveness of the target to the adversary is a key factor in determining the likelihood of an attack. Examples of issues that may be addressed here include:

- Proximity to a symbolic or iconic target, such as a national landmark
- Unusually high corporate profile among possible terrorists, such as a major defense contractor
- Any other variable not addressed elsewhere, when the SVA Team agrees it has an impact on the site's value as a target or on the potential consequences of an attack.

The SVA Team should use the best judgment of its subject matter experts to assess attractiveness. This is a subjective process as are all vulnerability assessments whether qualitative or quantitative in nature.

Each asset is analyzed to determine the factors that might make it a more or less attractive target to the adversary. Attractiveness is used to assess likelihood of the asset being involved in an incident.

Target Attractiveness is an assessment of the target's value from the adversary's perspective, which is one factor used as a surrogate measure for likelihood of attack. Note that target attractiveness itself includes the other factors of consequences and difficulty of attack/vulnerability. Target attractiveness is an aggregate of factors, which shows the complexity of the process of targeting and anti-terrorism efforts. Arguably target attractiveness is the dominant factor in determining terrorist risk. This is particularly true in the target-rich environment of the United States, where the rare nature of any particular terrorist act vs. the potential number of targets poses a major risk assessment dilemma.

The attractiveness of assets varies with the adversary threat including their motivation, intent, and capabilities. For example, the threat posed by an international terrorist and the assets they might be interested in could greatly vary from the threat and assets of interest to a violent activist or environmental extremist.

Figure 3.12 shows the factors that should be evaluated when evaluating target attractiveness for terrorism. The team can use these factors and rank each asset against each adversary by the scale shown in Figure 3.13. Other adversaries may be interested in other factors, and the user of the SVA is encouraged to understand the relevant factors and substitute them for those in Figure 3.12 as applicable.

### 3.5 SVA STEP 3: VULNERABILITY ANALYSIS

The Vulnerability Analysis step involves three steps, as shown in Figure 3.14. Once the SVA Team has determined how an event can be induced, it should determine how an adversary could make it occur. There are two schools of thought on methodology: the scenario-based approach and the asset-based approach. Both approaches are identical in the beginning, but differ in the degree of detailed analysis of threat scenarios and specific countermeasures applied to a given scenario. The assets are identified, and the consequences and target attractiveness are analyzed as per Step 2, for both approaches. Both approaches result in a set of annotated potential targets, and both approaches may be equally successful at evaluating security vulnerabilities and determining required protection.

Figure 3.11—Threat Rating Criteria

Threat Level	Description
<b>5 – Very High</b>	Indicates that a credible threat exists against the asset and that the adversary demonstrates the capability and intent to launch an attack, and that the subject or similar assets are targeted on a frequently recurring basis.
<b>4 – High</b>	Indicates that a credible threat exists against the asset based on knowledge of the adversary's capability and intent to attack the asset or similar assets.
<b>3 – Medium</b>	Indicates that there is a possible threat to the asset based on the adversary's desire to compromise similar assets.
<b>2 – Low</b>	Indicates that there is a low threat against the asset or similar assets and that few known adversaries would pose a threat to the assets.
<b>1 – Very Low</b>	Indicates no credible evidence of capability or intent and no history of actual or planned threats against the asset or similar assets.

Figure 3.12—Target Attractiveness Factors (for Terrorism)

<b>Type of effect:</b>
• Potential for causing maximum casualties
• Potential for causing maximum damage and economic loss to the facility and company
• Potential for causing maximum damage and economic loss to the geographic region
• Potential for causing maximum damage and economic loss to the national infrastructure
<b>Type of target:</b>
• Usefulness of the process material as a weapon or to cause collateral damage
• Proximity to national asset or landmark
• Difficulty of attack including ease of access and degree of existing security measures (soft target)
• High company reputation and brand exposure
• Iconic or symbolic target
• Chemical or biological weapons precursor chemical
• Recognition of the target

Figure 3.13—Attractiveness Factors Ranking Definitions (A)

Ranking Levels	Adversary Ranking (1 – 5)
1 – Very Low	Adversary would have no level of interest in the asset
2 – Low	Adversary would have some degree of interest in the asset
3 – Medium	Adversary would have a moderate degree of interest in attacking the asset
4 – High	Adversary would have a high degree of interest in the asset
5 – Very High	Adversary would have a very high degree of interest in the asset

Figure 3.14—Description of Step 3 and Substeps

Step	Task
<b>Step 3: Vulnerability Analysis</b>	
3.1 Define scenarios and evaluate specific consequences	Use scenario-analysis and/or use asset-based analysis to document the adversary's potential actions against an asset.
3.2 Evaluate effectiveness of existing security measures	Identify the existing measures intended to protect the critical assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary.
3.3 Identify vulnerabilities and estimate degree of vulnerability	Identify the potential vulnerabilities of each critical asset to applicable threats or adversaries. Estimate the degree of vulnerability of each critical asset for each threat-related undesirable event or incident and thus each applicable threat or adversary.

**Step 3.1—Define Scenarios and Evaluate Specific Consequences**

Each asset in the list of critical target assets from Step 2 is reviewed in light of the threat assessment, and the relevant threats and assets are paired in a matrix or other form of analysis, as shown in Attachment 1—Steps 3 – 5—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form. The importance of this step is to develop a design basis threat statement for each facility.

Once the SVA Team has determined how a malevolent event can be induced, it should determine how an adversary could execute the act.

The action in the Scenario-based approach follow the SVA method as outlined in Chapter 3. To establish an understanding of risk, scenarios can be assessed in terms of the severity of consequences and the likelihood of occurrence of security events. These are qualitative analyses based on the judgment and deliberation of knowledgeable team members.

**Step 3.2—Evaluate Effectiveness of Existing Security Measures**

The SVA Team will identify the existing measures intended to protect the critical assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary.

**Step 3.3—Identify Vulnerabilities and Estimate Degree of Vulnerability**

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and the subsequent destruction or theft of an asset. Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical security, or operational security practices.

For each asset, the vulnerability or difficulty of attack is considered using the definitions shown in Figure 3.15.

The Scenario-based approach is identical to the Asset-based approach in the beginning, but differs in the degree of detailed analysis of threat scenarios. The scenario-based approach uses a more detailed analysis strategy and brainstorms a list of scenarios to understand how the undesired event might be accomplished. The scenario-based approach begins with an onsite inspection and interviews to gather specific information for the SVA Team to consider.

The following is a description of the approach and an explanation of the contents of each column of the worksheet in Attachment 1—Steps 3 – 5 Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form.

Figure 3.15—Vulnerability Rating Criteria

Vulnerability Level	Description
<b>5 – Very High</b>	Indicates that there are no effective protective measures currently in place to Deter, Detect, Delay, and Respond to the threat and so an adversary would easily be capable of exploiting the critical asset.
<b>4 – High</b>	Indicates there are some protective measures to Deter, Detect, Delay, or Respond to the asset but not a complete or effective application of these security strategies and so it would be relatively easy for the adversary to successfully attack the asset.
<b>3 – Medium</b>	Indicates that although there are some effective protective measures in place to Deter, Detect, Delay, and Respond, there isn't a complete and effective application of these security strategies and so the asset or the existing countermeasures could likely be compromised.
<b>2 – Low</b>	Indicates that there are effective protective measures in place to Deter, Detect, Delay, and Respond, however, at least one weakness exists that an adversary would be capable of exploiting with some effort to evade or defeat the countermeasure given substantial resources.
<b>1 – Very Low</b>	Indicates that multiple layers of effective protective measures to Deter, Detect, Delay, and Respond to the threat exist and the chance that the adversary would be able to exploit the asset is very low.

The SVA Team devises a scenario based on their perspective of the consequences that may result from undesired security events given a postulated threat for a given asset. This is described as an event sequence including the specific malicious act or cause and the potential consequences, while considering the challenge to the existing countermeasures. It is conservatively assumed that the existing countermeasures are exceeded or fail in order to achieve the most serious consequences, in order to understand the hazard. When considering the risk, the existing countermeasures need to be assessed as to their integrity, reliability, and ability to deter, detect, and delay.

In this column the type of malicious act is recorded. As described in Chapter 2, the four types of security events included in the objectives of a SVA at a minimum include:

1. Theft/Diversion of material for subsequent use as a weapon or a component of a weapon
2. Causing the deliberate loss of containment of a chemical present at the facility
3. Contamination of a chemical, tampering with a product, or sabotage of a system
4. An act causing degradation of assets, infrastructure, business and/or value of a company or an industry.

Given the information collected in Steps 1 – 3 regarding the site's key target assets, the attractiveness of these targets, and the existing layers and rings of protection, a description of the initiating event of a malicious act scenario may be entered into the Undesired Event column. The SVA team brainstorms the vulnerabilities based on the information collected in Steps 1 – 3. The SVA team should brainstorm vulnerabilities for all of the malicious act types that are applicable at a minimum. Other scenarios may be developed as appropriate.

#### Completing the Worksheet

The next step is for the team to evaluate scenarios concerning each asset/threat pairing as appropriate. The fields in the worksheet are completed as follows:

1. **Asset:** The asset under consideration is documented. The team selects from the targeted list of assets and considers the scenarios for each asset in turn based on priority.
2. **Security Event Type:** This column is used to describe the general type of malicious act under consideration. At a minimum, the four types of acts previously mentioned should be considered as applicable.
3. **Threat Category:** The category of adversary including terrorist, activist, disgruntled employee, etc.
4. **Type:** The type of adversary category whether (I) – Insider, (E) – External, or (C) – Colluded threat.
5. **Undesired Act:** A description of the sequence of events that would have to occur to breach the existing security measures is described in this column.
6. **Consequences:** Consequences of the event are analyzed and entered into the Consequence column of the worksheet. The consequences should be conservatively estimated given the intent of the adversary is to maximize their gain.  
It is recognized that the severity of an individual event may vary considerably, so SVA teams are encouraged to understand the expected consequence of a successful attack or security breach.
7. **Consequences Ranking:** Severity of the Consequences on a scale of 1 – 5 as shown in Figure 3.8. The severity rankings are assigned based on a conservative assumption of a successful attack.



8. **Existing Countermeasures:** The existing security countermeasures that relate to detecting, delaying, or deterring the adversaries from exploiting the vulnerabilities may be listed in this column. The countermeasures have to be functional (i.e., not bypassed or removed) and sufficiently maintained as prescribed (i.e., their ongoing integrity can be assumed to be as designed) for credit as a countermeasure.
9. **Vulnerability:** The specific countermeasures that would need to be circumvented or failed should be identified.
10. **Vulnerability Ranking:** The degree of vulnerability to the scenario rated on a scale of 1 – 5 as shown in Figure 3.15.
11. **L(ikelihood):** The likelihood of the security event is assigned a qualitative ranking in the likelihood column. The likelihood rankings are generally assigned based on the likelihood associated with the entire scenario, assuming that all countermeasures are functioning as designed/intended. Likelihood is a team decision and is assigned from the Likelihood scale based on the factors of Vulnerability, Attractiveness, and Threat for the particular scenario considered.
12. **R(isk):** The severity and likelihood rankings are combined in a relational manner to yield a risk ranking. The development of a risk-ranking scheme, including the risk ranking values is described in Step 4.
13. **New Countermeasures:** The recommendations for improved countermeasures that are developed are recorded in the New Countermeasures column.

### 3.6 STEP 4: RISK ANALYSIS/RANKING

In either the Asset-based or the Scenario-based approach to Vulnerability Analysis, the next step is to determine the level of risk of the adversary exploiting the asset given the existing security countermeasures. Figure 3.16 lists the substeps.

The scenarios are risk-ranked by the SVA Team based on a simple scale of 1 – 5. The risk matrix shown in Figure 3.17 could be used to plot each scenario based on its likelihood and consequences. The intent is to categorize the assets into discrete levels of risk so that appropriate countermeasures can be applied to each situation.

Note: For this matrix, a Risk Ranking of “5 x 5” represents the highest severity and highest likelihood possible.

### 3.7 STEP 5: IDENTIFY COUNTERMEASURES:

A Countermeasures Analysis identifies shortfalls between the existing security and the desirable security where additional recommendations may be justified to reduce risk. In assessing the need for additional countermeasures, the team should ensure each scenario has the following countermeasures strategies employed:

- **DETER** an attack if possible
- **DETECT** an attack if it occurs
- **DELAY** the attacker until appropriate authorities can intervene
- **RESPOND** to neutralize the adversary, to evacuate, shelter in place, call local authorities, control a release, or other actions.

The SVA Team evaluates the merits of possible additional countermeasures by listing them and estimating their net effect on the lowering of the likelihood or severity of the attack. The team attempts to lower the risk to the corporate standard.

Figure 3.16—Description of Step 4 and Substeps

Step	Task
<b>Step 4: Risk Assessment</b>	
4.1 Estimate risk of successful attack	As a function of consequence and probability of occurrence, determine the relative degree of risk to the facility in terms of the expected effect on each critical asset (a function of the consequences or impacts to the critical functions of the facility from the disruption or loss of the critical asset, as evaluated in Step 1) and the likelihood of a successful attack (a function of the threat or adversary, as evaluated in Step 2, and the degree of vulnerability of the asset, as evaluated in Step 3).
4.2 Prioritize risks	Prioritize the risks based on the relative degrees of risk and the likelihoods of successful attacks.



Figure 3.17—Risk Ranking Matrix

L I K E L I H O O D	SEVERITY				
	5	4	3	2	1
	5			Med	Med
	4		Med	Med	Low
	3		Med	Low	Low
	2	Med	Med	Low	Low
	1	Med	Low	Low	Low

Figure 3.18—Description of Step 5 and Substeps

Step	Task
<b>Step 5: Countermeasures Analysis</b>	
5.1 Identify and evaluate enhanced countermeasures options	Identify countermeasures options to further reduce the vulnerabilities and thus the risks while considering such factors as: <ul style="list-style-type: none"> <li>• Reduced probability of successful attack</li> <li>• The degree of risk reduction provided by the options</li> <li>• The reliability and maintainability of the options</li> <li>• The capabilities and effectiveness of these mitigation options</li> <li>• The costs of the mitigation options</li> <li>• The feasibility of the options</li> </ul> Rerank to evaluate effectiveness.
5.2 Prioritize potential enhancements	Prioritize the alternatives for implementing the various options and prepare recommendations for decision makers

### 3.8 FOLLOW-UP TO THE SVA

The outcome of the SVA is:

- the identification of security vulnerabilities;
- a set of recommendations (if necessary) to reduce risk to an acceptable level.

The SVA results should include a written report that documents:

- The date of the study;
- The study team members, their roles and expertise and experience;
- A description of the scope and objectives of the study;
- A description of or reference to the SVA methodology used for the study;
- The critical assets identified and their hazards and consequences;
- The security vulnerabilities of the facility;
- The existing countermeasures;
- A set of prioritized recommendations to reduce risk.

Once the report is released, it is necessary for a resolution management system to resolve issues in a timely manner and to document the actual resolution of each recommended action.



## **Attachment 1—Example SVA Methodology Forms**

The following four forms can be used to document the SVA results. Blank forms are provided, along with a sample of how each form is to be completed. Other forms of documentation that meet the intent of the SVA guidance can be used.



Step 1: Critical Assets/Criticality Form		
Facility Name:		
Critical Assets Form		
Critical Assets	Criticality/Hazards	Asset Severity Ranking
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		



**Step 2: Attractiveness/Target Ranking Form**

Facility Name:

Critical Assets	Function/Hazards/ Criticality	Asset Severity Ranking	Asset Attractiveness					TR	
			Foreign/Domestic Attractiveness Rationale	A1	Employee/ Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale		A3
1.									
2.									
3.									
4.									
5.									
6.									

### Step 3 – 5: Vulnerability Analysis/Risk Ranking/Countermeasures Form

**Facility Name:**

**Critical Assets:**

**Attractiveness:**

[illegible]



## Glossary of Terms<sup>12</sup>

**Adversary:** Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. An adversary could include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, rogue employees, and private interests. Adversaries can include site insiders, site outsiders, or the two acting in collusion.

**Alert levels:** Describes a progressive, qualitative measure of the likelihood of terrorist actions, from negligible to imminent, based on government or company intelligence information. Different security measures may be implemented at each alert level based on the level of threat to the facility.

**Asset:** An asset is any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets in the SVA include the community and the environment surrounding the site.

**Asset category:** Assets may be categorized in many ways. Among these are:

- People
- Hazardous materials (used or produced)
- Information
- Environment
- Equipment
- Facilities
- Activities/Operations
- Company reputation

**Benefit:** Amount of expected risk reduction based on the overall effectiveness of countermeasures with respect to the assessed vulnerabilities.

**Capability:** When assessing the capability of an adversary, two distinct categories need to be considered. The first is the capability to obtain, damage, or destroy the asset. The second is the adversary's capability to use the asset to achieve their objectives once the asset is obtained, damaged, or destroyed.

**Checklist:** A list of items developed on the basis of past experience that is intended as a guide to assist in applying a standard level of care for the subject activity and to assist in completing the activity in as thorough a manner.

**Consequences:** The amount of loss or damage that can be expected, or may be expected from a successful attack against an asset. Loss may be monetary but may also include political, morale, operational effectiveness, or other impacts. The impacts of security events, which should involve those that are extremely severe. Some examples of relevant consequences in a SVA include fatality to member(s) of the public, fatality to company personnel, injuries to member(s) of the public, injuries to company personnel, large-scale disruption to public or private operations, large-scale disruption to company operations, large-scale environmental damage, large-scale financial loss, loss of critical data, and loss of reputation.

**Cost:** Includes tangible items such as money and equipment as well as the operational costs associated with the implementation of countermeasures. There are also intangible costs such as lost productivity, morale considerations, political embarrassment, and a variety of others. Costs may be borne by the individuals who are affected, the corporations they work for, or they may involve macroeconomic costs to society.

**Cost-Benefit analysis:** Part of the management decision-making process in which the costs and benefits of each countermeasure alternative are compared and the most appropriate alternative is selected. Costs include the cost of the tangible materials, and also the on-going operational costs associated with the countermeasure implementation.

**Countermeasures:** An action taken or a physical capability provided whose principal purpose is to reduce or eliminate one or more vulnerabilities. The countermeasure may also affect the threat(s) (intent and/or capability) as well as the asset's value. The cost of a countermeasure may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

**Countermeasures analysis:** A comparison of the expected effectiveness of the existing countermeasures for a given threat against the level of effectiveness judged to be required in order to determine the need for enhanced security measures.

**Cyber security:** Protection of critical information systems including hardware, software, infrastructure, and data from loss, corruption, theft, or damage.

**Delay:** A countermeasures strategy that is intended to provide various barriers to slow the progress of an adversary in penetrating a site to prevent an attack or theft, or in leaving a restricted area to assist in apprehension and prevention of theft.

**Detection:** A countermeasures strategy that is intended to identify an adversary attempting to commit a security event or other criminal activity in order to provide real-time observation as well as post-incident analysis of the activities and identity of the adversary.

**Deterrence:** A countermeasures strategy that is intended to prevent or discourage the occurrence of a breach of security by means of fear or doubt. Physical security systems such as warning signs, lights, uniformed guards, cameras, bars are examples of countermeasures that provide deterrence.

**Hazard:** A situation with the potential for harm.

**Intelligence:** Information to characterize specific or general threats including the motivation, capabilities, and activities of adversaries.

**Intent:** A course of action that an adversary intends to follow.

**Layers of protection:** A concept whereby several independent devices, systems, or actions are provided to reduce the likelihood and severity of an undesirable event.

**Likelihood of adversary success:** The potential for causing a catastrophic event by defeating the countermeasures. LAS is an estimate that the security countermeasures will thwart or withstand the attempted attack, or if the attack will circumvent or exceed the existing security measures. This measure represents a surrogate for the conditional probability of success of the event.

**Mitigation:** The act of causing a consequence to be less severe.

**Physical security:** Security systems and architectural features that are intended to improve protection. Examples include fencing, doors, gates, walls, turnstiles, locks, motion detectors, vehicle barriers, and hardened glass.

**Process Hazard Analysis (PHA):** A hazard evaluation of broad scope that identifies and analyzes the significance of hazardous situations associated with a process or activity.

**Response:** The act of reacting to detected or actual criminal activity either immediately following detection or post-incident.

**Risk:** The potential for damage to or loss of an asset. Risk, in the context of process security, is the potential for a catastrophic outcome to be realized. Examples of the catastrophic outcomes that are typically of interest include an intentional release of hazardous materials to the atmosphere, or the theft of hazardous materials that could later be used as weapons, or the contamination of hazardous materials that may later harm the public, or the economic costs of the damage or disruption of a process.

**Risk assessment:** Risk (R) assessment is the process of determining the likelihood of an adversary (T) successfully exploiting vulnerability (V) and the resulting degree of consequences (C) on an asset. A risk assessment provides the basis for rank ordering of risks and thus establishing priorities for the application of countermeasures.

**Safeguard:** Any device, system or action that either would likely interrupt the chain of events following an initiating event or that would mitigate the consequences.<sup>4</sup>

**Security layers of protection:** Also known as concentric 'rings of protection', a concept of providing multiple independent and overlapping layers of protection in depth. For security purposes, this may include various layers of protection such as counter-surveillance, counterintelligence, physical security, and cyber security.

**Security management system checklist:** A checklist of desired features used by a facility to protect its assets.

**Security plan:** A document that describes an owner/operator's plan to address security issues and related events, including security assessment and mitigation options. This includes security alert levels and response measures to security threats.

**Security Vulnerability Assessment (SVA):** A SVA is the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact. SVAs are not a quantitative risk analysis, but are performed qualitatively using the best judgment of security and safety professionals. The determination

of risk (qualitatively) is the desired outcome of the SVA, so that it provides the basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures.

**Target attractiveness:** An estimate of the value of a target to an adversary based on the factors shown below. Experience has shown that, particularly for terrorist attacks, certain targets better accomplish the objectives of the adversaries than do others. Since the SVA is a risk-based analytical approach, consideration must be given to these factors in defining the threat and in determining the need for any enhanced countermeasures.

- Potential for mass casualties/fatalities
- Extensive property damage
- Proximity to national assets or landmarks
- Possible disruption or damage to critical infrastructure
- Disruption of the national, regional or local economy
- Ease of access to target
- Media attention or possible interest of the media
- Company reputation and brand exposure

**Technical security:** Electronic systems for increased protection or for other security purposes including access control systems, card readers, keypads, electric locks, remote control openers, alarm systems, intrusion detection equipment, annunciating and reporting systems, central stations monitoring, video surveillance equipment, voice communications systems, listening devices, computer security, encryption, data auditing, and scanners.

**Terrorism:** The FBI defines terrorism as, "the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

**Threat:** Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

**Threat categories:** Adversaries may be categorized as occurring from three general areas:

- Insiders
- Outsiders
- Insiders working in collusion with outsiders

**Undesirable events:** An event that results in a loss of an asset, whether it is a loss of capability, life, property, or equipment.

**Vulnerabilities:** Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings, or operational and personnel practices.



## Abbreviations and Acronyms

A	Attractiveness
ACC	American Chemistry Council
AT	Target attractiveness
AIChE	American Institute of Chemical Engineers
API	American Petroleum Institute
AWCS	Accidental Worst-Case Scenario
C	Consequence
CCPS	Center for Chemical Process Safety of the American Institute of Chemical Engineers (AIChE)
CCTV	Closed Circuit Television
CEPPPO	Chemical Emergency Preparedness and Prevention Office (USEPA)
CMP	Crisis Management Plan
CSMS	Chemical Security Management System
CW	Chemical Weapons
CWC	Chemical Weapons Convention
D	Difficulty of Attack
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	U. S. Department of Transportation
EHS	Environmental, Health, and Safety
EPA	U. S. Environmental Protection Agency
ERP	Emergency Response Process
EHS	Environmental, Health, and Safety
FBI	U. S. Federal Bureau of Investigation
FC	Facility Characterization
HI	Hazard Identification
HSAS	Homeland Security Advisory System
IPL	Independent Protection Layer
IT	Information Technology
LA	Likelihood of Adversary Attack
LAS	Likelihood of Adversary Success
LOPA	Layer of Protection Analysis
MARSEC	Maritime Security Levels
MOC	Management of Change
NPRA	National Petrochemical and Refiners Association
OSHA	Occupational Safety and Health Administration
PHA	Process Hazard Analysis
PLC	Programmable Logic Controller
PSI	Process Safety Information
PSM	Process Safety Management (Also refers to requirements of 29 <i>CFR</i> 1910.119)
R	Risk
RMP	Risk Management Process (Also refers to requirements of EPA 40 <i>CFR</i> Part 68)
S	Severity of the Consequences
SOCMA	Synthetic Organic Chemical Manufacturers Association
SOP	Standard Operating Procedure
SVA	Security Vulnerability Assessment
T	Threat
TSA	Transportation Security Agency
V	Vulnerability
WMD	Weapons of Mass Destruction



## APPENDIX A—SVA Supporting Data Requirements

SVA Methodology Supporting Data	
Category*	Description
A	Scaled drawings of the overall facility and the surrounding community (e.g., plot plan of facility, area map of community up to worst case scenario radius minimum)
A	Aerial photography of the facility and surrounding community (if available)
A	Information such as general process description, process flow diagrams, or block flow diagrams that describes basic operations of the process including raw materials, feedstocks, intermediates, products, utilities, and waste streams
A	Information (e.g., drawings that identify physical locations and routing) that describes the infrastructures upon which the facility relies (e.g., electric power, natural gas, petroleum fuels, telecommunications, transportation [road, rail, water, air], water/wastewater)
A	Previous security incident information
A	Description of guard force, physical security measures, electronic security measures, security policies
A	Threat information specific to the company (if available)
B	Specifications and descriptions for security related equipment and systems. Plot plan showing existing security countermeasures
B	RMP information including registration and offsite consequence analysis (if applicable, or similar information)
B	Most up-to-date PHA reports for processes considered targets
B	Emergency response plans and procedures (site, community response, and corporate contingency plans)
B	Information on material physical and hazard properties (MSDS)
B	Crisis management plans and procedures (site and corporate)
B	Complete a SVA chemicals checklist to determine whether the site handles any chemicals on the following lists:
C	• EPA Risk Management Program (RMP) 40 CFR Part 68;
C	• OSHA Process Safety Management (PSM) 29 CFR 1910.119;
C	• Chemical Weapons Convention, Schedule 2 and specifically listed Schedule 3 chemicals;
C	• FBI Community Outreach Program (FBI List) for WMD precursors;
C	• The Australia Group list of chemical and biological weapons.
C	Design basis for the processes (as required)
C	Unit plot plans of the processes
C	Process flow diagrams (PFDs) and piping and instrument diagrams (P&IDs) for process streams with hazardous materials
C	Safety systems including fire protection, detection, spill suppression systems
C	Process safety systems including safety instrumented systems (SIS), PLC's, process control systems
C	Operating procedures for start-up, shutdown, and emergency (operators may provide general overview of this information, with written information available as required)
C	Mechanical equipment drawings for critical equipment containing highly hazardous chemicals
C	Electrical one-line diagrams
C	Control system logic diagrams
C	Equipment data information
C	Information on materials of construction and their properties
C	Information on utilities used in the process
C	Test and maintenance procedures for security related equipment and systems

\*Categories: A = Documentation to be provided to SVA team as much in advance as possible before arrival for familiarization;

B = Documentation to be gathered for use in SVA team meetings on site;

C = Documentation that should be readily available on an as-needed basis.





## APPENDIX B—SVA Countermeasures Checklist

### Appendix B Table of Contents

	Page
SVA Countermeasures Survey .....	47
IDENTIFICATION OF PHYSICAL SECURITY SYSTEMS .....	47
IDENTIFICATION OF PROCESS SAFETY SYSTEMS .....	47
SECURITY PROGRAM MANAGEMENT .....	48
(a) Security Organization .....	48
(b) Security Plans and Policies .....	48
(c) Security Resources .....	48
(d) Senior Management Security .....	48
(e) Security Audits .....	48
(f) Handling of Sensitive Information .....	49
(g) Internal Communications .....	49
THREAT DETECTION AND EVALUATION CAPABILITIES .....	50
(a) Threat Analysis Working Group .....	50
(b) Organization's Response to Threat Updates .....	51
PERIMETER BARRIERS – FENCES, GATES .....	52
(a) Fences .....	52
(b) Gates .....	52
(c) Vehicle Barriers .....	52
BUILDING BARRIERS – WALLS, ROOF/CEILING, WINDOWS, DOORS .....	53
(a) Walls .....	53
(b) Roof/Ceiling .....	53
(c) Windows .....	53
(d) Doors .....	54
INTRUSION DETECTION .....	55
(a) Intrusion Sensors (If Applicable) .....	55
(b) Intrusion Alarm Deployment (If Applicable) .....	55
(c) Intrusion Alarm Assessment .....	55
CLOSED CIRCUIT TELEVISION .....	55
(a) CCTV .....	55
ACCESS CONTROL .....	56
(a) Personnel Access .....	56
(b) Vehicle Access .....	56
(c) Contraband Detection .....	56
(d) Access Point Illumination .....	56
SECURITY FORCE .....	57
(a) Protective Force .....	57
(b) Local Law Enforcement Agencies .....	57
INFORMATION, COMPUTER, NETWORK, AND INTELLECTUAL PROPERTY SECURITY .....	58
(a) Information, Computer, Network, and Intellectual Property Security .....	58
PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS .....	60
(a) Hardening Processes .....	60
(b) Reducing the Quantity and Hazard of a Release from a Malicious Act .....	61
(c) Mitigating a Release from a Malicious Act .....	63
(d) Emergency Response, Crisis Management, and Community Coordination .....	64



### SVA Countermeasures Survey

The objective of the physical security portion of the survey is to identify measures that protect the entire facility and/or each critical asset of the facility, and to determine the effectiveness of the protection. This attachment contains checklists that are used to conduct the physical security portion of the survey. The Security Program Management Checklist is used to identify physical security measures that may be present to protect the entire facility or a critical asset at the facility. The remaining checklists are used to specifically evaluate the individual elements of the physical security system that are present. The conclusion of whether a particular element provides adequate protection is to be reported as part of the findings in the body of the SVA. A "set" of checklists should be completed for the facility as a whole and if appropriate, for each of the critical assets within the facility.

Note that the infrastructure interdependencies portion of the survey will identify infrastructures that support the facility and/or its critical assets (e.g., electric power, water, and telecommunications). A physical security review of these vital infrastructures should also be conducted.

#### IDENTIFICATION OF PHYSICAL SECURITY SYSTEMS

Date: [MONTH XX, 2002]

Facility: [FACILITY]

This checklist applies to [the entire facility/ASSET]

Instructions: This checklist identifies the physical security elements that may be used to protect the entire facility and/or a critical asset. Identify which elements are present for the facility or the critical asset listed above. Once physical security elements are identified, they can be reviewed by using the applicable checklists. At the completion of the reviews, the effectiveness of the elements is to be documented in the body of the survey report.

Physical Security System Element	Element Present		COMMENTS
	Yes	No	
Perimeter Barriers			
Building Barriers			
Intrusion Detection			
Access Controls			
Security Force			

#### IDENTIFICATION OF PROCESS SAFETY SYSTEMS

Date: [MONTH XX, 2002]

Facility: [FACILITY]

This checklist applies to [the entire facility/ASSET]

Instructions: This checklist identifies the process safety elements that may be used to protect the entire facility and/or a critical asset. Identify which elements are present for the facility or the critical asset listed above. Once physical security elements are identified, they can be reviewed by using the applicable checklists. At the completion of the reviews, the effectiveness of the elements is to be documented in the body of the survey report.

Process Safety System Element	Element Present		COMMENTS
	Yes	No	
Hardening Processes			
Emergency Response			
Chemical Detection			
Fire Detection			
Fire Suppression			

<b>SECURITY PROGRAM MANAGEMENT</b>	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
<b>COMMENTS</b>	
<b>(a) Security Organization</b>	
1. Is there a senior level security working group with representatives from each major office or department to establish security policies (including physical security, operations security, and infrastructure interdependencies security) and integrate them across all elements of the organization? <ul style="list-style-type: none"> <li>• If there is a senior level security working group, describe the membership, the lines of communication, and any scheduled periodic meetings to resolve security issues.</li> <li>• If there is not such a group, how are security policies established?</li> </ul>	
2. Is there a security office that is responsible for implementing security policies and procedures (including physical security, operations security, and infrastructure interdependencies security)? <ul style="list-style-type: none"> <li>• If there is a security office, where does it report in the organization, how many people are in the office, and are resources adequate? Also describe any training received.</li> <li>• If there is not such an office, how are security policies implemented?</li> </ul>	
<b>(b) Security Plans and Policies</b>	
3. Is there a mission statement describing the physical security, operations security, and infrastructure security programs?	
4. Is there a formal security plan and statement of security policies? If there is, describe it including how it is communicated to employees.	
5. Is there a formal threat definition and assessment statement? If there is, describe it including how it is communicated to employees.	
<b>(c) Security Resources</b>	
1. Are the resources (budget and staffing) applied to security (including physical security, operations security, and infrastructure interdependencies security) considered adequate?	
2. Do security personnel feel that they have adequate training to accomplish their functions?	
<b>(d) Senior Management Security</b>	
1. Is there an executive protection program for senior executives/managers? If there is such a program, describe it.	
2. Is public information on senior executives/managers controlled? If it is, describe how it is controlled.	
<b>(e) Security Audits</b>	
1. Is there a regular security assessment or audit? If there is, describe how it is done, by whom, and how frequently.	

2. Has the most recent audit indicated any weaknesses? Summarize the results of the audit, particularly any weaknesses identified.	
3. Have any corrective measures been implemented recently? Describe them.	
<b>(f) Handling of Sensitive Information</b>	
1. How is sensitive information identified and marked?	
2. Who has access to sensitive security information?	
3. How is sensitive information protected, stored, accessed, transmitted, and destroyed?	
4. How do senior executives/managers protect sensitive security information?	
<b>(g) Internal Communications</b>	
1. How does management provide security information to employees at the site?	
2. Describe the process for obtaining feedback from employees on security related issues.	

THREAT DETECTION AND EVALUATION CAPABILITIES	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to the entire facility	
COMMENTS	
<b>(a) Threat Analysis Working Group</b>	
1. Is the organization a member of a local threat analysis working group? Describe the group	
2. If the organization is a member of such a group, list the organizations that participate in the working group (e.g., local, county, state, and federal agencies, the military).	
3. Are there other industry partners participating in the working group? Describe them.	
4. Are active efforts being made to recruit other meaningful participants into the working group? Describe the efforts.	
5. Do the participants in the working group have management support, requirements, and funding to participate? Describe the situation.	
6. Are the members of the working group willing participants and do they work against bureaucratic obstacles that may prevent the success of the group? Describe the situation.	
7. Do the members of the working group have the authority to share information with other members of the group? Describe the situation.	
8. Have the members of the working group been given appropriate U.S. government clearances to share in threat information? Describe the situation.	
9. Do the members of the working group have access to the National Infrastructure Protection Center (NIPC), Analytical Services, Inc., (ANSER), FBI-sponsored InfraGuard, Carnegie Mellon University's CERT, and other information system security warning notices? List the threat information systems they use.	
10. Indicate the frequency and regularity of the working group meetings.	
11. Do the members of the working group have processes in place to obtain real-time information from the field (e.g., on-duty offices, civilian neighborhood watch programs, local businesses, other working groups in the area)? Describe these processes.	
12. Do members of the working group have the ability to initiate information-gathering requests back into the field environment? Describe the capability.	
13. Are the threat statements developed by the working group specific to the organization or the industry, versus general nationwide warnings? Describe the process for gathering these statements.	

14. Do some members of the working group conduct scheduled meetings with the public to discuss concerns and observations? Describe these interactions.	
15. Do the members of the working group know what the critical assets of the organization are? Describe the extent of their knowledge.	
16. Do the members of the working group understand industry interdependencies and work with other industry members to address these potential concerns? Describe the extent of these interactions.	
17. What are the roles and responsibilities of the working group members during response and recovery activities?	
<b>(b) Organization's Response to Threat Updates</b>	
1. Does senior management support and/or participate in the threat analysis working group? Describe the extent of the support/participation.	
2. Does the organization receive as-needed threat briefings from local, state, and federal agencies? Describe the nature and extent of the briefings.	
3. Does the organization have the ability to distribute organization-specific threat warnings in real time? Describe the process.	
4. Does the organization have the ability to augment security programs based on threat updates? Describe the process.	
5. Does the organization conduct historical trending analysis for security events (both planned and actual) and implement security activates to mitigate them? Describe the analysis.	
6. Does the organization create possible threat scenarios based on input from the threat analysis working group and conduct related security exercises? Describe the exercises.	

**PERIMETER BARRIERS—FENCES, GATES**

Date: [MONTH XX, 2002]

Facility: [FACILITY]

This checklist applies to [the entire facility/ASSET]

**COMMENTS****(a) Fences**

1. Characterize fence construction and rate the level of security it provides as low, moderate to high, or other (specify).

- Low: no fence or only a 6-foot chain-link fence.
- Moderate to high: 8-foot chain-link fence with outriggers, 10 to 12-foot chain-link fence, or over 12-foot chain-link fence with outriggers.

2. Characterize fence signage as no signs, posted "No Trespassing," or other (specify).

3. Characterize the fence alarm system as no alarms, fence sensors (taut wire, vibration, strain, electric field, or multiple sensors), or other (specify).

4. Fence area:

- Is the fence within 2 inches of firm hard ground?
- Is the fence line clear of vegetation, trash, equipment, and other objects that could impede observation?
- Is the area free of objects that would aid in traversing the fence?
- Is physical protection installed for all points where utilities (e.g., electric power lines, natural gas pipelines, telecommunication lines, water supply, storm sewers, drainage swells) intersect the fence perimeter?

5. How is the fence protected from vehicles (aircraft cable, concrete barriers or median, guard rails, steel posts, a ditch, crash I-beams, train barrier, or other [specify])?

6. Fence illumination:

- Is there security lighting for the fences? Describe the security lighting system.
- Do alarms or infrared detectors trigger the lighting? Describe the triggering process.

**(b) Gates**

1. Characterize the gates as no gate closure, vehicle bar, chain-link fence, or other (specify).

2. Characterize the gate locks as no lock, lock not used, gate unlocked, gate attended by personnel when unlocked, ID actuated lock, padlock, or other (specify).

3. How is access to gate keys controlled?

4. Gate lighting:

- Describe the security lighting for the gates.
- Do alarms or infrared detectors trigger the lighting? Describe the triggering process.

**(c) Vehicle Barriers**

1. Characterize vehicle barriers as none, a vehicle bar, blocked by vehicle when gate open, hydraulic wedge, or other (specify).



<b>BUILDING BARRIERS—WALLS, ROOF/CEILING, WINDOWS, DOORS</b>	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
<b>COMMENTS</b>	
<b>(a) Walls</b>	
2. Characterize wall construction and rate the level of security wall provide as low, moderate, or high. <ul style="list-style-type: none"> <li>• Low: chain-link mesh, 16-gauge metal, wood studs and dry wall, wood studs and plywood, or other (specify).</li> <li>• Moderate: clay block, 8-inch hollow block, 8-inch filled block, or other (specify).</li> <li>• High: 8-inch filled rebar block, 12-inch filled rebar block, 2-inch precast concrete tees, 4-inch reinforced concrete, 8-inch reinforced concrete, 12-inch reinforced concrete, 24-inch reinforced concrete, or other (specify).</li> </ul>	
3. Do the walls extend from the floor to the structural ceiling?	
<b>(b) Roof/Ceiling</b>	
1. Characterize the roof material and rate the level of security it provides as low, moderate, or high. <ul style="list-style-type: none"> <li>• Low: 20-gauge metal with insulation, ½-inch wood, or other (specify).</li> <li>• Moderate: 20-gauge metal built-up roof, concrete built-up roof with T-beams, or other (specify).</li> <li>• High: 5-½-inch concrete roof, 8-inch concrete roof, 3-foot earth cover, 3-foot soil/cement/earth cover, or other (specify).</li> </ul>	
2. Does the interior drop ceiling extend beyond the structural walls?	
<b>(c) Windows</b>	
1. Characterize the window materials and rate the level of security they provide as low or moderate. <ul style="list-style-type: none"> <li>• Low: standard windows or other (specify).</li> <li>• Moderate: 9-gauge expanded mesh, ½-inch diameter x 1-½-inch quarry screen, ½-inch diameter bars with 6-inch spacing, 3/16-inch x 2-½-inch grating, or other (specify).</li> </ul>	
2. Characterize the window alarms (for windows that would be accessible by foot or ladder) as none, vibration sensor, glass breakage sensor, conducting tape, grid mesh, multiple sensors, or other (specify).	

(d) Doors	
1. Characterize door materials and rate the level of security they provide as low, moderate, or high. <ul style="list-style-type: none"> <li>• Low: wood, 9-gauge wire mesh, hollow-core metal, no lock/hinge, or other (specify).</li> <li>• Moderate: hollow-core metal, tempered-glass panel, security-glass panel, half-height turnstile, or other (specify).</li> <li>• High security: ½-inch steel plate, turnstile – aluminum, Class V or VI vault, or other (specify).</li> </ul>	
2. Characterize the door locks and rate the level of security they provide as low, moderate, or high. <ul style="list-style-type: none"> <li>• Low: none, lock not used, or other (specify).</li> <li>• Moderate: door unlocked, attended by personnel when unlocked, ID actuated lock, padlock, keyed cylinder lock, combination lock, mechanically coded lock, or other (specify).</li> <li>• High: electronically coded lock, two-person rule lock system, lock inaccessible from the door exterior, or other (specify).</li> </ul>	
3. How is access to the keys for the door locks controlled?	
4. Door Alarms: <ul style="list-style-type: none"> <li>• Is door position monitored?</li> <li>• Indicate the type of door penetration sensor (vibration, glass breakage, conducting tape, grid mesh, or other [specify]).</li> </ul>	

<b>INTRUSION DETECTION</b>	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
<b>COMMENTS</b>	
<b>(a) Intrusion Sensors (If Applicable)</b>	
1. Characterize the exterior intrusion sensors as seismic buried cable, electric field, infrared, microwave, video motion, or other (specify).	
2. Characterize the interior intrusion sensors as sonic, capacitance, video motion, infrared, ultrasonic, microwave, or other (specify).	
<b>(b) Intrusion Alarm Deployment (If Applicable)</b>	
1. Characterize intrusions alarm deployment in terms such as: <ul style="list-style-type: none"> <li>• continuously monitored,</li> <li>• positioned to prevent gaps in coverage,</li> <li>• detection zone kept clear of obstructions (e.g., dips, equipment, snow, ice, grass, debris),</li> <li>• tamper and system problem indicators provided,</li> <li>• compensatory measures employed when alarms are not operating,</li> <li>• backup power provided, and</li> <li>• other (specify).</li> </ul>	
<b>(c) Intrusion Alarm Assessment</b>	
1. Characterize the assessment of intrusion alarms as not assessed, closed circuit TV, automatic deployment of protective force, or other (specify).	

<b>CLOSED CIRCUIT TELEVISION</b>	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
Note: Different access points to the facility and/or to critical assets may have different access controls. The comments should clearly distinguish whether the evaluation applies to all access points or to specific access points.	
<b>COMMENTS</b>	
<b>(a) CCTV</b>	
1. Describe the current CCTV system in use at the site.	
2. Characterize cameras in use and what asset(s) the cameras cover (PTZ, Autodome type, Fixed, Day/Night)	
3. Who monitors the CCTV cameras (Operations and/or Security) and what are the protocols for camera operation?	
4. Describe the policy for review of information recorded on CCTV system.	
5. Describe the preventive maintenance program for the CCTV system.	

<b>ACCESS CONTROL</b>	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
Note: Different access points to the facility and/or to critical assets may have different access controls. The comments should clearly distinguish whether the evaluation applies to all access points or to specific access points.	
<b>COMMENTS</b>	
<b>(a) Personnel Access</b>	
1. Characterize access point control as unmanned, unarmed guard, armed guard, or other (specify).	
2. Characterize the identification check process as none in place, casual recognition, credential check (e.g., drivers license, passport, state ID), picture badge, PIN, exchange badge, retinal scan, hand geometry, speech pattern, signature dynamics, fingerprint, or other (specify).	
3. Characterize the organization's badging policy in terms such as no badging policy, visitor badges required, badge issuance and control procedures in place (describe), and badges show permission to access specific areas (describe).	
<b>(b) Vehicle Access</b>	
1. Characterize vehicle access point controls as unmanned, unarmed guard, armed guard, or other (specify).	
2. Characterize the vehicle access identification process as none in place, vehicle stickers, vehicle stickers with personnel identification, automated system (describe), or other (specify).	
3. Describe the vetting process for incoming/outgoing bulk shipments of items by vehicle. Are deliveries scheduled or are is a list of drivers provided prior to delivery.	
<b>(c) Contraband Detection</b>	
1. Characterize item and vehicle search procedures as none, cursory, or detailed	
2. Is there a policy for incoming/outgoing drivers that report the possession of weapons? If so describe the policy/procedure.	
<b>(d) Access Point Illumination</b>	
1. Access Point Illumination: <ul style="list-style-type: none"> <li>Is there security lighting for the access points? Describe the security lighting system.</li> <li>Do alarms or infrared detectors trigger the lighting? Describe the triggering process.</li> </ul>	

SECURITY FORCE	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
COMMENTS	
<b>(a) Protective Force</b>	
1. Specify the size of the protective force in terms or total number and the number on duty during working hours, non-working hours, and weekends/holidays.	
2. Specify the equipment available to the protective force such as uniforms; vehicles (specify number); weapons (describe); communications devices (describe); and other equipment (describe).	
3. Describe the training of the protective force. Specifically, describe the initial training, any continuing training (e.g., on-the-job), and drills and exercises.	
4. Describe the organization of the protective force. Specifically, describe the command structure, their mission as defined, any established policies and procedures, and established emergency response plans.	
5. Are there provisions for a back-up force (e.g., recalling off-duty personnel)? Describe the provisions in place.	
6. Protective Force Command Center: <ul style="list-style-type: none"> <li>• Is there a protective force command and control center? Describe it.</li> <li>• Is there a backup center? Describe it.</li> </ul>	
7. Are protective force operations disguised to prevent intelligence about the facility from being inadvertently released? Describe how this is done.	
8. Describe protective force procedures for responding to alarms.	
9. Does the protective force provide security escort for visitors? Describe the nature of the escort.	
<b>(b) Local Law Enforcement Agencies</b>	
1. Describe the interaction of the protective force with local law enforcement agencies in terms of memoranda of agreement or other agreements in place (describe), protection responsibilities defined (describe), communication procedures developed (describe), and participation in drills and exercises.	
2. What is the approximate response time for local law enforcement personnel?	

INFORMATION, COMPUTER, NETWORK, and INTELLECTUAL PROPERTY SECURITY	
Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
COMMENTS	
<b>(a) Information, Computer, Network, and Intellectual Property Security</b>	
1. Have steps been taken to protect technical and business information that could be of use to potential adversaries (sometimes referred to as operational security or OPSEC)?	
2. Have the documentation/computer files that need to be protected for confidentiality been systematically identified and regularly backed-up?	
3. Is sensitive information in research and development and laboratory areas safeguarded against inadvertent disclosure?	
4. Is sensitive information in maintenance areas safeguarded against inadvertent disclosure?	
5. Are computers as well as disks, tapes, and other media adequately secured physically from theft?	
6. Are procedures followed to reduce the likelihood that spoken information (in face-to-face conversations, phone calls, and radio communications) could be picked up by adversaries?	
7. If the content of radio communications cannot be restricted for operational reasons, have they been voice-encrypted?	
8. Are user authorizations granted on the basis of "need to know," "least access," and "separation of functions" rather than position or precedent (note: this has to be balanced against the process safety concepts of employee access to process safety information and employee participation)?	
9. Are appropriate procedures followed for protecting and destroying sensitive documents that could provide key information on critical process operation or vulnerabilities?	
10. Is the computer/server room secured?	
11. Is the computer/server room on the second floor (to protect it from flooding and to reduce the likelihood of theft), and away from outside walls?	
12. Is the computer/server room equipped with adequate communications capability?	
13. Is access to the computer/server room limited to only authorized personnel who need entry?	
14. Are appropriate hardware, software, and procedural techniques used for protecting computers and networks, such as:	
a. Firewalls?	
b. User ID?	

c. Password controls, including the regular changing of passwords?	
d. Encryption?	
15. Virus protection?	
16. Are computer transaction histories periodically analyzed to look for irregularities that might indicate security breaches?	
17. Is Internet access disabled in all application software or operating systems that are pre-packaged?	
18. Are measures in place to control access to or otherwise secure process-specific operating information (e.g., including diagrams, procedures, control loop/DCS information), both electronic and hardcopy versions?	
19. Are process control systems protected from external manipulation (e.g., hacking into control system to operate equipment or delete or alter software codes)?	
20. Is access to process control systems via the Internet or Intranet been restricted? If access is allowed, is the access allowed only to the absolute minimum number of personnel necessary, using user ID, password, separate authentication, and encryption controls as appropriate?	
21. Are temporary passwords restricted from use except for new employees, or when a password is forgotten or is inactive?	
22. Are vendor-supplied passwords changed immediately after installation?	
23. Do users have screen saver with password available and in use when leaving computers on and unattended?	

<b>PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS</b>	
Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
<b>COMMENTS</b>	
<b>(a) Hardening Processes</b>	
1. Have existing security countermeasures been designed using the concept of rings of protection? Are the critical assets that may qualify as attractive targets at the center of concentric rings of layered protective features?	
2. Have process and systems been designed using the concept of layers of protection? Are there adequate independent protective layers that would detect, prevent, or mitigate a release of hazardous materials?	
3. Are critical process areas and equipment protected with traffic barriers, bollards, dikes, or other measures (e.g., diversionary structures that prevent vehicles from accelerating along a clear path to the process/equipment) to prevent ramming with vehicles?	
4. Are process "unit roads or streets" (i.e., roadways that provide access into specific process areas) provided with gates and, if so, are they securely closed when not in use (these gates may help limit direct vehicular access to critical equipment)?	
5. Are vehicles (except necessary material transport vehicles and/or authorized plant vehicles) prohibited from parking near critical process equipment (300 feet is considered a minimum distance)?	
6. Are full tank trailers or rail cars containing highly hazardous materials (i.e., those materials that could be targeted by terrorists) stored away from fence lines or perimeter areas to reduce their vulnerability to attack?	
7. Are full tank trailers or rail cars containing flammable or explosive materials stored away from critical process areas and equipment to prevent propagation of effects to critical processes?	
8. Are critical processes or equipment, such as tanks storing highly hazardous materials, protected from explosion or fire at adjacent processes (e.g., blast walls)?	
9. Is good housekeeping practiced in critical process areas and are trash dumpsters or receptacles located away from critical processes and equipment (trash dumpsters and poor housekeeping may make it easier to hide a bomb)?	
10. Are doors to interior buildings (e.g., process buildings) and control rooms locked or otherwise secured, where appropriate?	



11. Are hinge pins on doors to critical process areas on the inside of the door? (Note: May not be possible and still maintain easy egress in fire/emergency situations—doors must open out.)	
12. Are critical process areas surrounded with locked and secure fencing (in addition to site perimeter fencing) or located within locked buildings? (Note: Locked and secured fencing or buildings may create confined space issues.)	
13. If critical process areas are not surrounded by fencing or within buildings or if infeasible to do so, are the processes patrolled or monitored continuously by security personnel?	
14. Are highly reactive materials (e.g., water-reactive chemicals) stored in a location and manner that minimizes the potential for intentional contamination (e.g., stored in locked building away from water hose connections, situated away from pipelines/connections with potential incompatible chemicals)?	
15. Are key valves, pumps, metering stations, and open-ended lines on critical processes, especially those in remote or uncontrolled/unrestricted areas, locked closed, located in locked secure structures (e.g., pump house), surrounded by locked secure fencing, and/or constructed of heavy-duty, tamper-resistant materials?	
16. Are ingredients for products potentially targeted for contamination unloaded, stored, transferred, and added to the process in a manner that is monitored and checked?	
17. Can exposed/remote equipment on critical processes feasibly be re-located to more secure/less vulnerable locations?	
18. Can critical process equipment that is highly recognizable from the ground and/or site perimeter be made less recognizable? (Note: This must be balanced against emergency responders need to readily identify equipment)	
19. Can critical processes or equipment be recognized readily from the air (consult aerial photos, if available) and, if so, can they be made less recognizable? (Note: This must be balanced against safety and code issues, such as painting of certain storage tanks in light colors.)	
<b>(b) Reducing the Quantity and Hazard of a Release from a Malicious Act</b>	
1. Has a review of site utility systems been conducted to identify and assess vulnerability of utilities that are essential to safe operation and shutdown of critical processes? Examples of possible critical utilities are:	

a. Electrical power	
b. Cooling water	
c. Compressed air	
d. Natural gas or other fuels	
e. Steam	
f. Nitrogen or other inert gases	
g. Secondary containment (drainage and sewer systems)	
h. Communications systems	
2. Are utility areas that can affect critical processes appropriately secured and monitored? (e.g., cooling water systems and agitation systems on reactive chemical processes that may be particularly important)	
3. Where appropriate, has safe and rapid manual shutdown capability been provided for critical processes and utilities?	
4. Where loss or reduction of utilities can potentially lead to uncontrolled reactions on critical processes, is the operating status of the utilities monitored and/or to alert personnel (e.g., an alarm sounds when cooling water flow is lost or reduced below critical levels)?	
5. Where loss or reduction of utilities can potentially lead to uncontrolled reactions on critical processes, are feed systems interlocked to agitation, cooling systems, and other appropriate utilities in the event of loss of those utilities or systems?	
6. Are appropriate back-up power supplies available for critical processes to allow a safe shutdown? (Note: UPS can be compromised by adversaries.)	
7. In the event of loss of power or pneumatics, do valves and other equipment fail to a safe position in critical processes?	
8. Are container storage areas secured or otherwise monitored, especially those outside of process buildings or in remote areas? (Note: A fire or explosion involving multiple containers can lead to smoke/combustion by-products that present offsite hazards and can serve as a diversion or a "statement.")	
9. Have storage and process inventories of hazardous chemicals been reduced to the extent practicable?	
10. Where appropriate, are critical processes containing highly hazardous chemicals "segmented" (either automatically or via manual action) to prevent release of the majority of process contents (i.e., only the quantity in the compromised "segment" would be released)?	
11. Are pipelines containing highly hazardous materials equipped with low-pressure interlock systems that shut valves or take other action to minimize the release quantity?	

12. Are open-ended lines or other lines or vessel drain systems on critical processes equipped with excess flow valves?	
13. Where appropriate, are hazardous materials being procured in smaller containers instead of maintaining large inventories in a single vessel?	
14. Has a review been conducted to determine if hazardous materials can be purchased and used in a less hazardous form? (Note: This may be particularly applicable to solvents/carriers and waste or water treatment chemicals.)	
15. If materials can be purchased and used in less hazardous forms, is this approach being addressed in an expedited manner?	
16. Has the feasibility and merit of storing large inventories of highly hazardous materials in underground tanks or other systems (e.g., aboveground vaults) that would limit the release rate been evaluated? (Note: This must be balanced against environmental concerns and other liabilities.) If found to be of merit, are plans in place to pursue this approach?	
17. Where appropriate and feasible, are tanks, vessels, and tank trailers/rail cars disconnected from delivery or transfer piping when not in use? (Note: The piping may be more vulnerable than the vessel.)	
<b>(c) Mitigating a Release from a Malicious Act</b>	
1. Are appropriate passive mitigation systems in-place for addressing large volume releases from critical processes?	
2. Have passive mitigation systems been assessed for integrity (i.e., are they being tested and/or maintained as required periodically) and vulnerability to be compromised?	
3. Has passive leak-limiting technology been used where possible (e.g., gaskets resistant to blowout, excess flow valves, etc.)?	
4. Are appropriate active mitigation systems in-place for addressing large volume releases at critical processes?	
5. Have active mitigation systems been assessed for integrity (i.e., are they being tested and/or maintained as required periodically) and vulnerability to be compromised?	
6. Are key control valves, pumps, and other equipment associated with active mitigation systems been locked or secured in operational/ready positions or located within secure structures?	
7. Has expanding the areas of the site where potential ignition sources are limited or eliminated (e.g., expanding the area of site subject to Class I/Div 1 or 2 electrical classification) been evaluated?	

14. Are local police, fire departments, health care providers, and other emergency responders aware of the hazardous materials at the site?	
15. Are plans in place to communicate information to local offsite emergency responders and officials in the event of a release?	
16. Do periodic emergency drills address malicious acts or other security-related emergencies?	
17. Is there a drill/exercise critique system in place to assure that experience from drills and actual emergencies are incorporated into the emergency response plan?	

## APPENDIX C— SVA Interdependencies and Infrastructure Checklist

### Appendix C Table of Contents

	Page
INTERDEPENDENCIES TABLES .....	71
INFRASTRUCTURE OVERSIGHT AND PROCEDURES .....	72
(a) Infrastructure Oversight.....	72
(b) Infrastructure Procedures .....	72
INTERNAL ELECTRIC POWER SUPPLY AND DISTRIBUTION SYSTEM .....	73
(a) Primary Source of Electric Power.....	73
(b) Electric Distribution System .....	73
(c) Backup Electric Power Systems .....	73
INTERNAL HVAC SYSTEM .....	74
(a) Primary HVAC System .....	74
(b) Supporting Infrastructures .....	74
(c) Backup HVAC Systems .....	73
INTERNAL TELEPHONE SYSTEMS .....	75
(a) Primary Telephone System .....	75
(b) Data Transfer .....	75
(c) Cellular/Wireless/Satellite Systems .....	75
INTERNAL MICROWAVE/RADIO COMMUNICATIONS SYSTEM .....	76
(a) On-site Fixed Components .....	76
(b) Mobile and Remote Components .....	76
INTERNAL INTRANET AND E-MAIL SYSTEM .....	77
(a) Contained within a Larger System .....	77
(b) Separate System .....	77
(c) Access .....	78
INTERNAL COMPUTERS AND SERVERS .....	79
(a) Electric Power Sources .....	79
(b) Environmental Control .....	79
(c) Protection .....	79
INTERNAL FIRE SUPPRESSION AND FIRE FIGHTING SYSTEM .....	80
(a) Alarms .....	80
(b) Fire Suppression .....	80
(c) Fire Fighting .....	80
(d) Other Systems .....	80
INTERNAL SCADA SYSTEM .....	81
(a) Type of System .....	81
(b) Control Centers .....	81
(c) Electric Power Sources .....	81
(d) Communications Pathways .....	82
(e) Remote Components .....	82
(f) Dedicated SCADA Computers and Servers .....	83
INTERNAL DOMESTIC WATER SYSTEM .....	84
(a) Primary System .....	84
(b) External Water Supply System .....	84
(c) Internal Water Supply System .....	84
(d) Backup System .....	85
INTERNAL INDUSTRIAL WATER/WASTEWATER SYSTEM .....	86
(a) Primary Water System .....	86
(b) External Water Supply System .....	86
(c) Internal Water Supply System .....	86
(d) Backup Water System .....	87
(e) Primary Industrial Wastewater System .....	87
(f) Backup Wastewater System .....	88

FACILITY ENGINEERING .....	109
(a) Responsibilities .....	109
(b) Facility Engineering Information .....	109
(c) Public Access to Facility .....	109
FACILITY OPERATIONS .....	110
(a) Responsibilities .....	110
(b) Facility Operations Control .....	110
(c) Facility Construction, Repair, and Maintenance .....	110
ADMINISTRATIVE SUPPORT ORGANIZATIONS .....	111
(a) Procurement .....	111
(b) Legal .....	111
(c) Budget and Finance .....	111
(d) Marketing .....	111
(e) Internal Information .....	111
TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY .....	112
(a) Telecommunications .....	112
(b) Information Technology .....	112
PUBLICLY RELEASED INFORMATION .....	113
(a) Responsibilities .....	113
(b) General Procedures .....	113
(c) Report Release .....	113
(d) Press Contacts .....	113
(e) Briefing and Presentations .....	113
(f) Public Testimony .....	113
(g) Internet Information .....	113
TRASH AND WASTE HANDLING .....	114
(a) Responsibilities .....	114
(b) Trash Handling .....	114
(c) Paper Waste Handling .....	114
(d) Salvage Material Handling .....	114
(e) Dumpster Control .....	114

**INTERDEPENDENCIES TABLES****INTERNAL AND EXTERNAL INFRASTRUCTURES TO BE INCLUDED**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

(Note: Not all infrastructures supporting each asset/facility need to be included in this survey. Only those infrastructures that are important to the asset's/facility's ability to continue to carry out its critical functions and activities need be considered in detail. In addition, the time and resources allotted for the survey may limit the infrastructures that can be examined.)

INFRASTRUCTURE	YES	NO	RATIONALE FOR EXCLUSION/INCLUSION
<b>Internal</b>			
Electric Power Supply and Distribution System			
HVAC System			
Telephone System			
Microwave/Radio Communications System			
Intranet and E-mail System			
Computers and Servers			
Fire Suppression/ Fire Fighting System			
SCADA System			
Domestic Water System			
Industrial Water System			
Physical Security System			
Human Resources Support			
Financial System			
<b>External</b>			
Electric Power			
Natural Gas			
Petroleum Fuels			
Telecommunications			
Water and Wastewater			
Road Transportation			
Rail Transportation			
Air Transportation			
Water Transportation			

**INTERNAL ELECTRIC POWER SUPPLY AND DISTRIBUTION SYSTEM**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Primary Source of Electric Power</b>	
If the primary source of electric power is a commercial source, are there multiple independent feeds? If so, describe the feeds and their locations.	
If the primary source of electric power is a system operated by the facility or asset, what type of system is it?	
If a facility operated primary electric generation system is used, what is the fuel or fuels used?	
If petroleum fuel is used, what quantity of fuel is stored on site for the primary electric generation system and how long it will last under different operating conditions?	
If the fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?	
<b>(b) Electric Distribution System</b>	
Are the components of the electric system that are located outside of buildings (such as generators, fuel storage facilities, transformers, transfer switches) protected from vandalism or accidental damage by fences or barriers? If so, describe the type of protection and level of security it provides.	
Are the various sources of electric power and the components of the internal electric distribution systems such that they may be isolated for maintenance or replacement without affecting the critical functions of the asset/facility? If not, describe the limitations.	
Have any single points of failure been identified for the electrical power supply and distribution system? If so, list them and describe.	
<b>(c) Backup Electric Power Systems</b>	
Are there additional emergency sources of electric supply beyond the primary system (such as multiple independent commercial feeds, backup generators, uninterruptible power supply [UPSs])? If there are, describe them.	
If there is a central UPS, does it support all the critical functions of the asset/facility in terms of capacity and connectivity? Specify for how long it can operate on battery power and list any potentially critical functions that are not supported.	
If there is a backup generator system, does it support all the critical functions of the facility in terms of capacity and connectivity? Specify the fuel and list any potentially critical functions that are not supported.	
Is the fuel for the backup generator system a petroleum fuel? If yes, specify the quantity stored on site and how long it will last.	
If the fuel is stored on site, are arrangements and contracts in place for resupply and management of the fuel?	



### INTERNAL TELEPHONE SYSTEMS (Including Voice, FAX, and Data Transfer)

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Primary Telephone System</b>	
What types of telephone systems are used within the asset/facility? Are there multiple independent telephone systems? Specify the types of systems, their uses, and whether they are copper-wire or fiber-optic based.	
If there are multiple independent telephone systems within the asset/facility, is each one adequate to support the critical functions and activities? Indicate any limitations.	
If there are multiple (from independent systems) or redundant (from built-in backups) switches and cables, are they physically separated and isolated to avoid common causes of failure?	
Are the telephone switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify types of protection provided.	
<b>(b) Data Transfer</b>	
For large volume and high-speed data transfer within the asset/facility, is there a separate system of switches and cables within the asset/facility? Specify the type of system and whether it is copper-wire or fiber-optic based.	
If there is a separate system for large-volume and high-speed data transfer, are there redundant switches and cables? If yes, describe the situation.	
If there are redundant switches and cables, are they physically separated and isolated to avoid common causes of failure?	
Are the data-transfer switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify the types of protection provided.	
<b>(c) Cellular/Wireless/Satellite Systems</b>	
Are cellular/wireless telephones and pagers in widespread use within the asset/facility? If yes, briefly describe their uses.	
If cellular/wireless telephones and pagers are in widespread use, are they adequate to support the critical functions and activities? Specify any limitations.	
Are satellite telephones or data links in widespread use within the asset/facility? If yes, briefly describe their uses.	
If satellite telephones or data links are in widespread use, are they adequate to support the critical functions and activities? Specify any limitations.	

**INTERNAL INTRANET AND E-MAIL SYSTEM**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Contained within a Larger System</b>	
Is the asset's/facility's intranet and e-mail system dependent on the asset's/facility's computers and servers? If yes, describe the dependence.	
Is the asset's/facility's intranet and e-mail system dependent on the asset's/facility's telephone system? If yes, describe the dependence.	
<b>(b) Separate System</b>	
If the asset's/facility's intranet and e-mail system is a separate system, are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the intranet and e-mail system? If yes, specify under what conditions and for how long.	
If the asset's/facility's intranet and e-mail system is a separate system, does it have its own backup electric power supply, such as local UPSs? If yes, specify the type and how long it can operate.	
If the asset's/facility's intranet and e-mail system is a separate system, does the asset's/facility's central HVAC system provide environmental control for important components or does it have its own independent environmental control system? If it has its own, specify the type.	
If the asset's/facility's intranet and e-mail system is a separate system, can it operate with a loss of all environmental control? If yes, specify for how long under various conditions.	
If the asset's/facility's intranet and e-mail system is a separate system, are there any backup environmental controls explicitly for the system? If yes, indicate the type of backup and the expected maximum duration of operation.	
If the asset's/facility's intranet and e-mail system is a separate system, is there special physical security provided for the important components? If yes, specify the type of security and the level of protection provided.	
If the asset's/facility's intranet and e-mail system is a separate system, is there special fire suppression equipment for the important components such as Halon, Inergen, inert gases, or carbon dioxide? If yes, specify the type of system.	
If the asset's/facility's intranet and e-mail system is a separate system, are there special features or equipment in the area of the important components to limit flooding or water intrusion? If yes, indicate the precautions taken.	

### INTERNAL COMPUTERS AND SERVERS (Including Mainframes, Firewalls, and Router Equipment)

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Electric Power Sources</b>	
Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the computers and servers? If yes, indicate under what conditions and for how long.	
Do the computers and servers have their own backup electric power supply (such as local UPSs or generators)? If yes, specify the types of backup and how long they can operate.	
<b>(b) Environmental Control</b>	
Does the asset's/facility's central HVAC system provide environment control to the computer and server areas or do the computer and server areas have their own independent environmental control system? If they have their own system, specify the type.	
Can the computers and servers operate with a loss of all environmental control? If yes, specify for how long under various conditions.	
Are there any backup environmental controls explicitly for the computer and server areas? If yes, indicate the type of backup and the expected maximum duration of operation.	
<b>(c) Protection</b>	
Is there special physical security provided for the computer and server areas? If yes, specify the type of security and the level of protection provided.	
Is there special fire suppression equipment in the computer and server areas such as Halon, Inergen, inert gases, or carbon dioxide? If yes, specify the type.	
Are there special features or equipment in the computer and server areas to limit flooding or water intrusion? If yes, describe them.	
Are there alarms for the computer and server areas for such things as unauthorized intrusion, loss of electric power, loss of environmental control, fire, and flooding or water intrusion? If yes, specify the types of alarms, how they are monitored, and the response procedure.	

## INTERNAL SCADA SYSTEM

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Type of System</b>	
Does the asset/facility make use of a substantial SCADA system (i.e., one that covers a large area or a large number of components and functions)? If yes, indicate what functions are monitored and/or controlled, the type of system, and the extent of the system.	
Is the SCADA system independent of the asset's/facility's primary electric power supply and distribution system?	
Is the SCADA system independent of the asset's/facility's telephone system?	
Is the SCADA system independent of the asset's/facility's microwave or radio communications system?	
Is the SCADA system independent of the asset's/facility's computers and servers?	
<b>(b) Control Centers</b>	
Where is the primary control center for the SCADA system located?	
Is there a backup control center? If yes, where is it located? Is it sufficiently remote from the primary control center to avoid common causes of failure such as fires, explosions, or other large threats?	
Are there backups to the SCADA computers and servers at the backup control center or at some other location? If yes, indicate the location of the backup computers and servers, whether they are completely redundant or cover only the most critical functions, and whether they are active "hot" standbys or have to be activated and initialized when needed.	
Note: The following sets of questions on electric power sources and communications pathways apply to the control centers as well as the other components of the SCADA system.	
<b>(c) Electric Power Sources</b>	
Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the SCADA system? If yes, indicate the types.	
If there is a special UPS, does it support all the functions of the SCADA system in terms of capacity? Specify for how long it can operate on battery power.	
If there is a special backup generator system, does it support all the functions of the SCADA system in terms of capacity?	
What is the fuel or fuels used by the special SCADA backup generator system? If stored on site, specify the quantity stored and how long it will last.	

Are there backup environmental controls for these remote components? If yes, indicate the type of backup, the fuels used, and the expected length of operations.	
Is physical security provided for the remote components of the special SCADA radio communications system? If yes, specify the types of security and the level of protection provided.	
Are there alarms at the remote components of the special SCADA radio communications system for such things as intrusion, loss of electric power, loss of environmental control, and fuel reserves? If yes, specify the types of alarms, how they are monitored, and to the response procedure.	
<b>(f) Dedicated SCADA Computers and Servers</b>	
Are there provisions within the asset's/ facility's primary electric power supply and distribution system to supply power for the special dedicated SCADA computers and servers? If yes, specify under what conditions and for how long.	
Do the special dedicated SCADA computers and servers have their own backup electric power supply, such as local UPSs? If yes, specify the types and how long they can operate.	
Does the asset's/facility's central HVAC system provide environment control for the separate special SCADA computer and server areas?	
How long can the separate dedicated SCADA computers and servers operate with a loss of all environmental control? Indicate the conditions that could affect the length of time.	
Do the separate dedicated SCADA computer and server areas have their own independent environmental control system? If yes, specify the type.	
Are there any backup environmental controls explicitly for the dedicated SCADA computer and server areas? If yes, indicate the type of backup and the expected maximum duration of operation.	
Is there special physical security provided for the separate SCADA computer and server areas? If yes, specify the type of security and the level of protection provided.	
Is there special fire suppression equipment in the separate dedicated SCADA computer and server areas such as Halon, Inergen, inert gases, or carbon dioxide? If yes, specify the type of system.	
Are there special features or equipment in the separate SCADA computer and server areas to limit flooding or water intrusion? If yes, indicate the precautions taken.	
Are there alarms for the separate SCADA computer and server areas for such things as unauthorized intrusion, loss of electric power, loss of environmental control, fire, and flooding or water intrusion? If yes, specify the types of alarms, how they are monitored, and the response procedure.	

Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site domestic water system pumps? If yes, specify them.	
If there is a special UPS, can it support the on-site domestic water system pumps at required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the on-site domestic water system pumps at the required levels? Also indicate the type of fuel or fuels used.	
If the fuel for the dedicated backup generator system for the on-site domestic water system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
<b>(d) Backup System</b>	
Is there an independent backup water source to the primary domestic supply system? If yes, specify the type of backup system (such as wells, river, reservoir, tank truck), describe the specific source of the water, indicate the adequacy of the backup supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric).	
Are the independent backup water source system pumps independent of the asset's/facility's primary electric power supply and distribution system?	
Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the backup water source system pumps? If yes, specify them.	
If there is a special UPS, can it support the backup domestic water source pumps at the required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the backup domestic water source system pumps at the required levels? Also indicate the type of fuel or fuels used.	
If the fuel for the dedicated backup generator system for the backup water source system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	

Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the on-site industrial water system pumps? If yes, specify them.	
If there is a special UPS, can it support the on-site industrial water system pumps at required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the on-site industrial water system pumps at the required levels? Also indicate the type of fuel or fuels.	
If the fuel for the dedicated backup generator system for the on-site industrial water system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
<b>(d) Backup Water System</b>	
Is there an independent backup water source to the primary industrial water supply system? If yes, specify the type of backup system (such as wells, river, reservoir, tank truck), describe the specific source of the water, indicate the adequacy of the backup supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric).	
Are the independent backup water source system pumps independent of the asset's/facility's primary electric power supply and distribution system?	
Are there multiple sources of electric supply (such as multiple independent commercial feeds, backup generators, UPSs) explicitly for the backup water source system pumps? If yes, specify them.	
If there is a special UPS, can it support the backup industrial water source pumps at the required levels? Specify for how long it can operate on battery power.	
If there is a special backup generator system, can it support the backup industrial water source system pumps at required levels? Also indicate the type of fuel or fuels.	
If the fuel for the dedicated backup generator system for the backup water source system pumps is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
<b>(e) Primary Industrial Wastewater System</b>	
Does the asset/facility have an on-site industrial wastewater system? If yes, specify the types of wastewater that are processed and the processes used.	
Are the on-site industrial wastewater lift pumps independent of the asset's/facility's primary electric power supply and distribution system?	

**INTERNAL PHYSICAL SECURITY SYSTEM**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Electric Power Sources</b>	
Are the asset's/facility's monitoring and alarm systems normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e., is the asset's/facility's primary electric power supply and distribution system the primary electric power source)?	
Are there multiple sources of electric power for the monitoring and alarm systems? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, UPSs, or batteries dedicated to support the monitoring and alarm systems. Specify what electric power sources are in place.	
If there is a special UPS, can it support all the functions of the monitoring and alarm systems in terms of capacity? Specify for how long it can operate on battery power.	
If there is a special generator system, can it support all the functions of monitoring and alarm systems in terms of capacity? Also indicate the type of fuel or fuels used.	
If the fuel for the special security generator system is a petroleum fuel, indicate the quantity stored on site and how long it will last. Are arrangements and contracts in place for resupply and management of the fuel?	
<b>(b) Communications Pathways</b>	
Are the asset's/facility's monitoring and alarm systems normally dependent upon the asset's/facility's telephone system?	
Are there multiple independent telephone systems or dedicated switches and cables supporting the monitoring and alarm systems? This could consist of the asset's/facility's telephone system and its backup or redundant systems; or combinations of multiple independent telephone systems or dedicated communications lines. Specify the types of systems used and whether they are copper-wire or fiber optic-cable based.	
Are the redundant telephone systems or switches and cables physically separated and isolated to avoid common causes of failure? If not, indicate any potential points of common failure.	



Are there multiple independent computers supporting the monitoring and alarm systems? This could consist of the asset's/facility's main computers and servers and their backup or redundant systems, or combinations of multiple independent computers. Specify the type of computers used.	
Are there multiple sources of electric power for any computers dedicated to support the monitoring and alarm systems? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the monitoring and alarm systems. If yes, specify the type and how long they can operate.	
Does the asset's/facility's central HVAC system provide environment control for the separate dedicated computers for the monitoring and alarm systems?	
How long can the separate dedicated computers of the monitoring and alarm systems operate with a loss of all environmental control? Indicate the conditions that could affect the length of time.	
Do the separate dedicated computers for the monitoring and alarm systems have their own independent environmental control system? If yes, specify the type.	
Are there backup environmental controls explicitly for any dedicated computers of the monitoring and alarm systems? If yes, indicate the type of backup and the expected maximum duration of operation.	

Are the dedicated telephone switches and data-transfer switches that support the human resources offices and functions located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify the type of protection.	
<b>(c) Computer Support</b>	
Are the asset's/facility's human resources offices and functions normally dependent upon the facility's main computers and servers?	
Are there multiple independent computers supporting the human resources offices and functions? This could consist of the asset's/facility's main computers and servers and their backup or redundant systems, or combinations of multiple independent computers. Specify the type of computers used.	
Are there multiple sources of electric power for any computers dedicated to support the human resources offices and functions? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support human resources. If yes, specify the type and how long they can operate.	
Does the asset's/facility's central HVAC system provide environment control for any separate dedicated computers that support the human resources offices and functions?	
How long can the separate dedicated computers that support the human resources offices and functions operate with a loss of any environmental control? Indicate the conditions that could affect the length of time.	
Do the separate dedicated computers that support the human resources offices and functions have their own independent environmental control system? If yes, specify the type.	
Are there backup environmental controls explicitly for any dedicated computers that support the human resources offices and functions? If yes, indicate the type of backup and the expected maximum duration of operation.	

Are the dedicated telephone switches and data-transfer switches that support the financial systems and functions located in a limited access or secured area away from potential damage due to weather or water leaks? If so, specify the type of protection.	
<b>(c) Computer Support</b>	
Are the asset's/facility's financial systems and functions normally dependent upon the facility's main computers and servers?	
Are there multiple independent computers supporting the financial systems and functions? This could consist of the facility's main computers and servers and their backup or redundant systems, or combinations of multiple independent computers. Specify the type of computers used.	
Are there multiple sources of electric supply for any computers dedicated to support the financial systems and functions? This could consist of the asset's/facility's primary electric power supply and distribution system and its backup or redundant systems; or combinations of multiple independent commercial electric feeds, backup generators, or UPSs dedicated to support the financial systems and functions. If yes, specify the type and how long they can operate.	
Does the asset's/facility's central HVAC system provide environment control for any separate dedicated computers that support the financial systems and functions?	
How long can the separate dedicated computers that support the financial systems and functions operate with a loss of any environmental control? Indicate the conditions that could affect the length of time.	
Do the separate dedicated computers that support the financial systems and functions have their own independent environmental control system? If so, specify the type.	
Are there any backup environmental controls explicitly for the dedicated computers that support the financial systems and functions? If yes, indicate the type of backup and the expected maximum duration of operation.	

**EXTERNAL NATURAL GAS INFRASTRUCTURE**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Sources of Natural Gas</b>	
How many city gate stations supply the natural gas distribution system in the area of the asset/facility and the asset/facility itself? If more than one, which ones are critical to maintaining the distribution system?	
How many distinct independent transmission pipelines supply the city gate stations? Indicate if an individual gate station is supplied by more than one transmission pipeline and which stations are supplied by independent transmission pipelines.	
<b>(b) Pathways of Natural Gas</b>	
Do the distribution pipelines from the individual city gate stations follow independent pathways to the area of the asset/facility? If not, specify how often and where they intersect or follow the same corridor.	
Are the paths of the pipelines co-located with the rights-of-way of other infrastructures? If yes, indicate how often and where they follow the same rights-of-way and the infrastructures that are co-located.	
Are the paths of the pipelines located in areas susceptible to natural or accidental damage (such as across bridges or dams, in earthquake or landslide areas)? If yes, indicate the locations and types of potential disruptions.	
Is the local distribution system well integrated (i.e., can gas readily get from any part of the system to any other part of the system)?	
<b>(c) Natural Gas Contracts</b>	
Does the asset/facility have a firm delivery contract, an interruptible contract, or a mixed contract with the natural gas distribution company or the transmission companies? Specify the companies involved and whether there is a direct physical link (pipeline) to each company.	
If there is an interruptible contract (even in part), what are the general conditions placed up interruptions such as the minimum quantity that is not interruptible, the maximum number of disruptions per time period, and the maximum duration of disruptions? Has natural gas service been interrupted in the past? If yes, describe the circumstances and any effect the outages have had on the critical functions and activities of the asset/facility.	

**EXTERNAL PETROLEUM FUELS INFRASTRUCTURE**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Uses of Petroleum Fuels</b>	
Are petroleum fuels used in normal operations at the asset/facility? If yes, specify the types and uses.	
Are petroleum fuels used during contingency or emergency operations such as for backup equipment or repairs? If yes, specify the types of fuels and their uses.	
<b>(b) Reception Facilities</b>	
How are the various petroleum fuels normally delivered to the asset/facility? Indicate the delivery mode and normal frequency of shipments for each fuel type.	
Under maximum use-rate conditions, are there sufficient reception facilities (truck racks, rail sidings, surge tank capacity, barge moorings) to keep up with maximum contingency or emergency demand? If no, explain where the expected shortfalls would be and their impacts.	
Are the petroleum fuel delivery pathways co-located with the rights-of-way of other infrastructures or located in areas susceptible to natural or accidental damage (across bridges or dams, in earthquake or landslide areas)? If yes, indicate the locations and types of potential disruptions.	
Are contingency procedures in place to allow for alternative modes or routes of delivery? If yes, describe these alternatives and indicate whether they have sufficient capacity to fully support the critical functions and activities of the asset/facility.	
<b>(c) Supply Contracts</b>	
Are contracts in place for the supply of petroleum fuels? Specify the contractors, the types of contracts, the modes of transport (pipeline, rail car, tank truck), and the frequency of normal shipments.	
Are arrangements for emergency deliveries of petroleum fuels in place? Indicate the basic terms of the contracts in terms of the maximum time to delivery and the minimum and maximum quantity per delivery. Also, indicate if these terms are such that there may be effects on the critical functions and activities of the asset/facility.	

Historically, have the internet and dedicated data transfer systems in the area been reliable? Quantify in terms of number of both complete outages and dropped connections.	
Typically, when internet or data transfer connectivity outages or disruptions occur, are they of significant duration (as opposed to just a few seconds or minutes)? Quantify in terms of potential effects on the critical functions and activities at the asset/facility.	
<b>(d) Backup Communications Systems</b>	
Are there redundant or backup telephone systems in place if the primary system is disrupted? Specify the extent to which the secondary systems can support the critical functions and activities at the asset/facility.	
Are there redundant or backup internet and dedicated data transfer systems in place if the primary systems are disrupted? Specify the extent to which the secondary systems can support the critical functions and activities at the asset/facility.	

**EXTERNAL ROAD TRANSPORTATION INFRASTRUCTURE**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Road Access</b>	
Are there multiple roadways into the area of the asset/facility from the major highways and interstates? Describe the route or routes and indicate any load or throughput limitations with respect to the needs of the asset/facility.	
Are there any choke points or potential hazard areas along these roadways such as tunnels, bridges, dams, low-lying fog areas, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, closures have occurred somewhat regularly.	
<b>(b) Road Access Control</b>	
Could intruders or others determined to do damage to the asset/facility gain access to the asset/facility or nearby areas by road without being readily identified and controlled? If yes, describe the means of access and indicate any limitations on the number of people, the size and number of vehicles, and the size or quantity of material that could approach the asset/facility by road.	
Are there uncontrolled parking lots or open areas for parking near the facility where vehicles could park without drawing significant attention? If yes, indicate the number of vehicles and the size or types of vehicles that would begin to be noticed.	

**EXTERNAL AIR TRANSPORTATION INFRASTRUCTURE**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset: \_\_\_\_\_

COMMENTS	
<b>(a) Airports and Air Routes</b>	
Are there multiple airports in the area of the site of sufficient size and with sufficient service to support the critical functions and activities at the asset/facility? Enumerate the airports and indicate any limitations.	
Are there any regular air routes that pass over or near the asset/facility that could present a danger to the asset/facility if there were some sort of an air disaster? Record any concerns.	



**EXTERNAL PIPELINE TRANSPORTATION INFRASTRUCTURE**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist applies to:

Entire Facility

Critical Asset \_\_\_\_\_

COMMENTS	
<b>(a) Pipeline Access</b>	
What materials feedstocks or products (such as crude oil, intermediate petroleum products, refined petroleum products, or liquefied petroleum gas—do not include water, wastewater, or natural gas unless there are special circumstances related to these items) are supplied to or shipped from the asset/facility by way of pipeline transportation?	
Are there multiple pipelines and pipeline routes into the area of the asset/facility from major interstate transportation pipelines? If yes, indicate which pipelines or combinations of pipelines have sufficient capacity to serve the asset/facility.	
List the pipeline owners/operators, indicate the types of service provided (dedicated or scheduled shipments), describe the route or routes, and indicate any capacity limitations with respect the needs of the asset/facility.	
Are there any bottlenecks or potential hazard areas along these pipelines or pipeline routes such as interconnects, terminals, tunnels, bridges, dams, landslide areas, or earthquake faults? Describe the constrictions or hazards and indicate if, historically, outages or delays have occurred somewhat regularly.	
<b>(b) Pipeline Access Control</b>	
Could intruders or others determined to bring down the asset/facility gain access to the pipeline near the asset/facility or elsewhere along the pipeline route? Describe the protective measures that are in place and indicate any pipeline segments or facilities (such as pump stations, surge tanks) of concern.	

**FACILITY ENGINEERING**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This section covers security issues related to the engineering information related to the facility. Included are the facility design, configuration, and layout; utility service systems; building floor plans; etc.

COMMENTS	
<b>(a) Responsibilities</b>	
What organization(s) is responsible for facility engineering?	
<b>(b) Facility Engineering Information</b>	
What facility engineering information (e.g., engineering drawings, site maps, utility service lines, floor plans, entry paths into the facility, etc.) is available?	
What organization(s) has control of this information?	
What other internal organizations are allowed access to this information?	
What external organizations (e.g., fire department, environmental agency) have been given access to this information?	
Is any of the facility engineering information publicly available?	
Can sensitive information be gleaned from commercial overhead imaging (e.g., aerial photography, commercial satellite images)? If yes, describe.	
How is this information protected?	
Is this information on the computer system or network?	
How is the information disposed of when no longer needed?	
<b>(c) Public Access to Facility</b>	
Are tours allowed of any or all of the facility? If yes, describe what portions of the facility are open and who is allowed to tour.	
Is any portion of the facility open to the public or special interest groups? If yes, describe.	
Are periodic meetings held where outsiders are allowed inside the facility? If yes, describe.	
Are there procedures for security escorting of visitors? If yes, describe.	

**ADMINISTRATIVE SUPPORT ORGANIZATIONS**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

<b>COMMENTS</b>	
<b>(a) Procurement</b>	Purchasing and procurement activities including: Generating Need (e.g., requisition or RFP), Selecting Supplier, Documenting the Purchase, Providing Delivery of Item or Service, Payment.
What organization(s) is responsible for reviewing procurement activities from a security perspective?	
What is the process used to review RFPs, contracts, and other procurement documents for security-related information?	
How is the procurement information protected before release? Include documents, files, copiers, facsimiles, computer files?	
Is security-sensitive information uniquely marked, both on paper and electronically? If yes, describe how.	
How is security-sensitive procurement information destroyed?	
How are company credit cards controlled? Who is authorized to have one? How is security-related information from credit card use identified and protected?	
<b>(b) Legal</b>	
What organization(s) is responsible for reviewing legal department activities from a security perspective?	
How are legal documents (e.g., patents, environmental impact statements, safety reports, Securities and Exchange Commission filings, Federal Energy Regulatory Commission filings, etc.) reviewed for security implications?	
How are these documents protected?	
<b>(c) Budget and Finance</b>	
What organization(s) is responsible for reviewing budget and finance activities from a security perspective?	
How are budget and finance documents reviewed for security implications?	
How are these documents protected?	
<b>(d) Marketing</b>	
What organization(s) is responsible for reviewing marketing activities from a security perspective?	
How are marketing materials reviewed for security implications?	
How are these documents protected?	
<b>(e) Internal Information</b>	
Are there policies and procedures for handling "Internal Use Documents" (e.g., memos, notes, newsletters, etc.)? If yes, describe.	
How are these documents protected?	
How are these documents destroyed when no longer needed?	

**PUBLICLY RELEASED INFORMATION**

Date: \_\_\_\_\_ Facility: \_\_\_\_\_

This checklist covers information that is released to the public via corporate communications, press releases, the Internet, and other means.

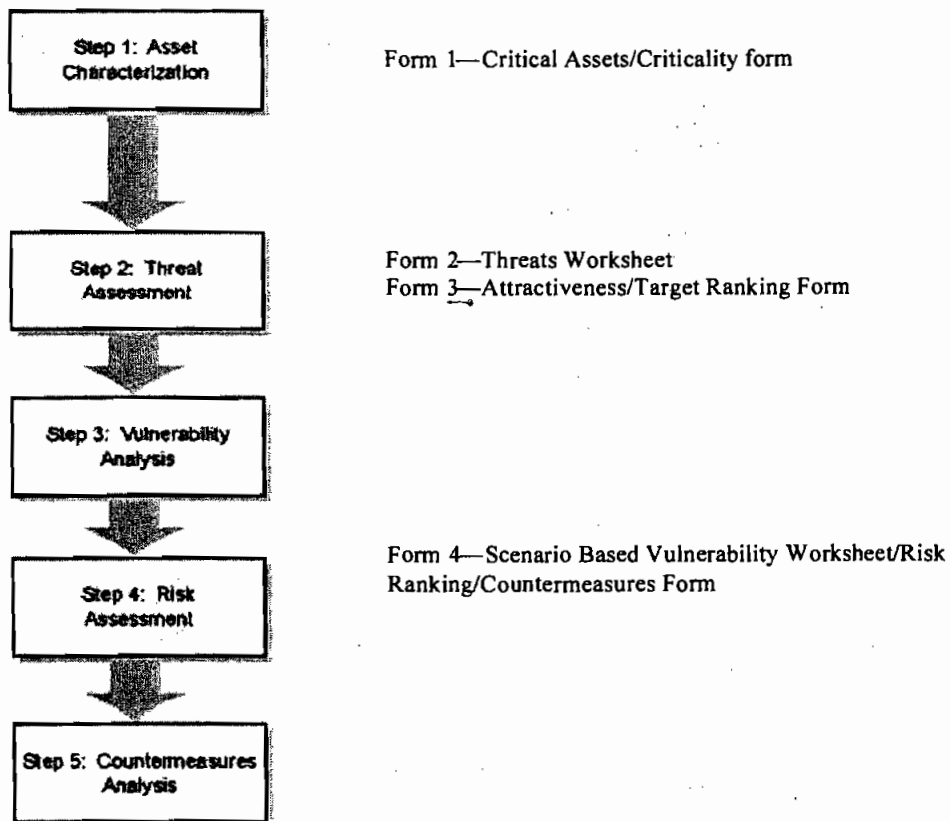
COMMENTS	
<b>(a) Responsibilities</b>	
What organization(s) is responsible for reviewing information (from a security perspective) that is to be released to the public?	
<b>(b) General Procedures</b>	
What is the process used to review information before release?	
How is the information protected before release? Include documents, files, copiers, facsimiles, computer files.	
<b>(c) Report Release</b>	
Who is responsible for reviewing reports released by the company?	
Who generates the reports?	
What type of information is included?	
What is the distribution and ultimate disposition of company-released reports?	
<b>(d) Press Contacts</b>	
Are specific people designated to interact with the press?	
How are they trained (including training on security issues)? Who trains them?	
<b>(e) Briefing and Presentations</b>	
Are briefings and presentations to be given by company employees reviewed for security issues? If yes, describe how.	
<b>(f) Public Testimony</b>	
Is public testimony that is to be given by company employees reviewed for security issues? If yes, describe how.	
<b>(g) Internet Information</b>	
Is there a policy in place to review information posted on the company Internet site for security issues? If yes, describe.	
Who reviews information before it is posted on the Website?	
Is the Website reviewed and monitored regularly for security-related information? If so, describe how.	

## Appendix C1—Refinery SVA Example

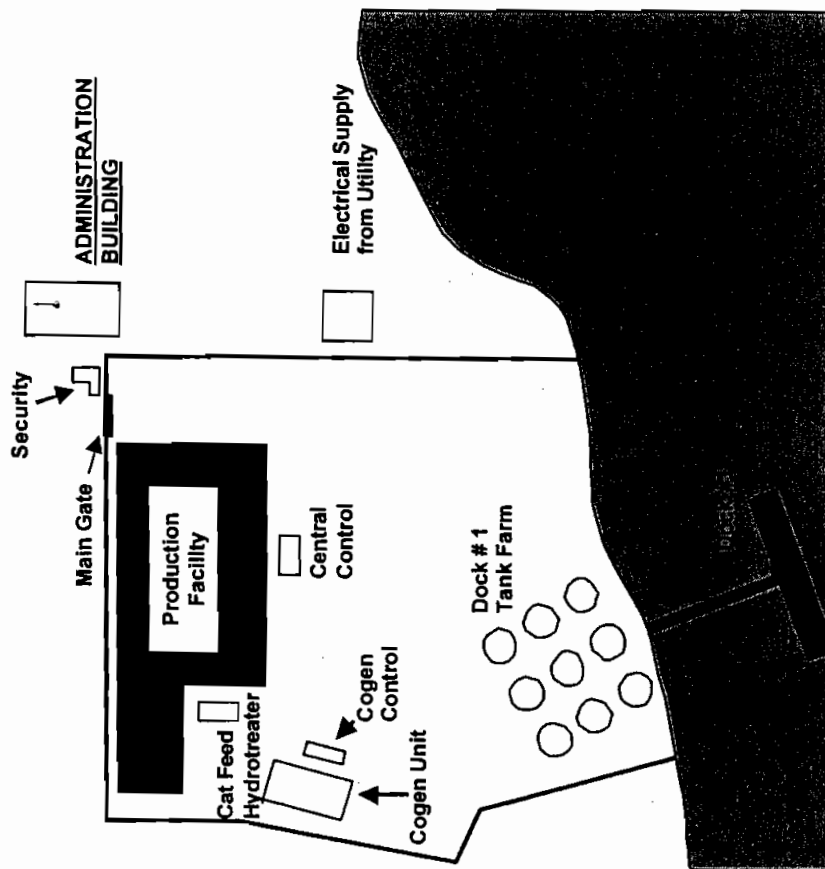
The application of the SVA Methodology to a fictitious refinery is illustrated in the following example. Only the first page of each of the four forms is shown for illustrative purposes. It is assumed that the study is conducted by the refinery company and considers the various interfaces with customers and suppliers. However, the security of the customer and supplier facilities is the responsibility of the owners of those facilities.

The study is conducted in a top-down, systematic manner following the logic flowchart for the SVA as shown in Figure A. The five steps of the process are documented in four forms:

Figure A—SVA Methodology Flow Diagram



## Fictitious Refinery Example



## Form 2: Threats Worksheet

Facility Name: Fictitious Refinery

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Assumed Adversary Capability	Adversary Motivation	Threat Ranking
1. Terrorist	EXT	No specific group or threat to the refinery	<ul style="list-style-type: none"> <li>- General industry terrorist threats only</li> <li>- HSAS Yellow as of the time of the SVA</li> </ul>	<ul style="list-style-type: none"> <li>- Use explosives or small arms to destroy target</li> <li>- May be interested in theft of products of value to terrorist organizations for secondary attack</li> </ul>	<ul style="list-style-type: none"> <li>- Use of improvised explosive device possibly involving a vehicle is most likely scenario</li> <li>- Assume trained, with good information and significant resources to plan and execute attack</li> </ul>	Assume highly motivated to cause maximum damage to critical infrastructure and casualties	4
2. Disgruntled employee or contractor	INT	Employees and contractors	<ul style="list-style-type: none"> <li>- Company facilities have had telephone bomb threats</li> <li>- No actual damage but threats have been made.</li> <li>- Assume general industry experience with insider sabotage is credible</li> </ul>	<ul style="list-style-type: none"> <li>- Might cause intentional overfill of tank or damage to equipment leading to release; might cause product contamination; possible for explosion</li> <li>- Possible for workplace violence</li> <li>- Potential for theft</li> </ul>	<ul style="list-style-type: none"> <li>- Specialized insider knowledge and training</li> <li>- Unrestricted access to entire facility</li> <li>- Not likely to use weapons if sabotage but may use small arms if workplace violence</li> </ul>	Potential for disgruntled employee due to disciplinary action; other workplace violence reasons; possibly in collusion with outside terrorist group in extreme case	3
3. Activist	EXT	Citizens for Green Environment has expressed interest	Multiple demonstrations have occurred at the plant	<ul style="list-style-type: none"> <li>- Possibly interested in causing public embarrassment; temporary shutdown of plant; long range goal of elimination of toxic substance in use.</li> </ul>	<ul style="list-style-type: none"> <li>- Highly organized; well funded to cause staged attack of multiple facility operations simultaneously (dock, rail, gate)</li> </ul>	Highly politically charged and motivated	4

## Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures

Facility Name: Fictitious Refinery

Critical Assets: 20. Dock 1

Scenario Worksheet Form											
Security Event Type	Threat Category	Type	Undesired Act	Consequences	S	Existing Countermeasures	Vulnerability	Vulnerability Ranking	L	R	New Countermeasures
1.1. Loss of containment	Terrorist	I/E	Attack on vessel or dock facility by way of an improvised explosive device	Damage to barge and dock facilities; loss of logistics for feedstock and products; major environmental release; fire and explosion; possible to shutdown channel	S5	1.1. USCG boat patrols of the channel and port 1.2 Roving guardforce	1.1. Lack of access control from water, 1.2 Low lighting 1.3No intrusion detection	5	L4		Consider improving lighting, access control, monitoring by CCTV, and administrative controls per requirements of Enclosure 2 of NVIC 11-02.



## Appendix C2—Fictitious Pipeline Example

The application of the SVA Methodology to a fictitious petroleum liquids pipeline system is illustrated in the following example. Only the first page of each of the four forms is shown for illustrative purposes. It is assumed that the study is conducted by the pipeline company and considers the various interfaces with customers and suppliers. However, the security of the customer and supplier facilities is the responsibility of the owners of those facilities.

The general approach is to apply risk assessment resources and, ultimately, special security resources primarily where justified based on the SVA results. The SVA process involves consideration of the pipeline system from both the general viewpoint and specific asset viewpoint. Consideration at the general level is useful for determination of overall impacts of loss, infrastructure and interdependencies at the system level. The benefit of evaluating specific assets is that individual risks can be evaluated and specific countermeasures applied where justified in addition to more general countermeasures.

For example, all facilities will maintain a minimum level of security with general countermeasures such as the pipeline shutdown and control strategies and administrative security controls. Certain assets will justify a more specific level of security based on their value and expected level of interest to adversaries.

The SVA methodology uses this philosophy in several ways. The method is intended to be comprehensive and systematic in order to be thorough. First, it begins with the SVA team gaining an understanding of the entire pipeline system, the assets that comprise the pipeline system, the critical functions of the pipeline, and the hazards and impacts if these assets or critical functions are compromised. This results in an understanding of which assets and functions are “critical” to the business operation. Criticality may be defined both in terms of the potential impact to the workers, community, the environment and the company, as well as to the business importance and continuity of the system. For example, a pumping station or a specific branch along the pipeline system may be a critical part of the operation of the pipeline system due to inability to operate without it or, if attacked, it has the greatest impact. As such it may be given a high priority for further analysis and special security countermeasures.

Based on this first level of screening from all assets to critical assets, a critical asset list is produced. Next, the critical assets are reviewed in light of the threats. Adversaries may have different objectives, so the critical asset list is reviewed from each adversary’s perspective and an asset attractiveness ranking is given. This factor is a quick measure of whether the adversary would value damaging, compromising, or stealing the asset, which serves as an indicator of the likelihood that an adversary would want to attack this asset and why.

If an asset is both critical (based on value and consequences) and attractive, then it is considered a “target” for purposes of the SVA. A target may optionally receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities. As shown in Figure A, all assets receive at least a general security review. This is accomplished by the basic SVA team’s consideration as an asset to begin with, along with a baseline security survey. General security considerations may be found in security references such as the countermeasures checklist provided in Appendix F.

The study is conducted in a top-down, systematic manner following the logic flowchart for the SVA as shown in Figure A. The five steps of the process are documented in four forms:

**Form 3—Attractiveness/Target Ranking Form**

Columns 1 – 3 are repeated from Form 1 for reference. Column 4 is a documented rationale for why the particular asset is attractive (or unattractive) and Column 5 is a ranking of that attractiveness on a relative Attractiveness Ranking scale or equivalent. This is repeated for other adversaries. Column 10 is an overall Target Ranking per the same scale, and is normally considered to be the highest attractiveness of any of the individual adversary rankings but also considers that the sum the different adversary's interests may make the asset more attractive. The Target Ranking is used to judge the degree of attractiveness of the target considering all the adversaries.

**Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form**

Column 1 is the Security Event Type (generally one of four security events including loss of containment, degradation of the asset, theft, or contamination); Column 2 is the Threat Category (adversary type such as terrorist, activist, employee); Column 3 is the Type of Adversary Attack (Insider/External); Column 4 is the Undesired Act (the assumed attack scenario, generally taken from the Threats Worksheet Columns 5, 6, 7); Column 5 is the Consequences; Column 6 (S) is the Severity Ranking from the Severity Ranking scale; Column 7 is the Existing Countermeasures, which considers the Deter, Detect, Delay, and Respond philosophy; Column 8 is the Vulnerability, which also considers the weaknesses or missing elements of the security strategy specific to the scenario; Column 9 is the Vulnerability Ranking per the Vulnerability Ranking scale; Column 10 is the Likelihood ranking (L) using the Likelihood scale, which is a judgment of the team considering the factors of Vulnerability, Threat, and Attractiveness; Column 11 is the Risk ranking (R) per the referenced Risk Ranking Matrix values; and Column 12 is the New /Countermeasures suggestions (where the risk is considered significant enough to justify the need for change).

**Responsibilities**

This example includes a sampling of assets that may be owned or operated by various parties. The responsibilities for conducting the SVA and for providing security need to be determined and may not solely be with the pipeline owner/operator. It is recommended that the SVA include the appropriate parties to fully analyze the security issues, and that the results are discussed with owner/operators of adjacent facilities and infrastructure providers as required for risk communication and completeness.

## Form 1: Critical Assets/Criticality Form

Facility Name: 1. Fictitious Pipeline Company

Critical Assets Form			Asset Severity Ranking
Critical Assets	Criticality/Hazards		
1. Main Line, 24-inch Liquids Pipeline System—1000 miles, provides 500,000 b/d. Finished products; Gasoline, Jet Fuel and home heating oil. 35 main-line block valves (approximately every 50 miles), 20 booster (pumping) stations, traverses primarily rural areas.	Main line serves large metropolitan areas. Several million retail customers plus 5 major international airports, and two large military installations. Includes a major above ground river crossing, which provides drinking water to large urban community.		5
2. ABC Branch—10 miles, 8 inch branch line serving mixed products to marketing terminal serving a rural population.	Serves rural customer base. No national defense impact. Remotely located and no major environmental impacts. Alternative delivery sources available.		1
3. DEF Branch and inter-modal terminal—Branch line providing mixed products to multi-modal marketing terminal, breakout facility, interconnection to other pipelines and direct connect to military, commercial airports and power plant.	Possible onsite fatalities. Possible offsite environmental impact. Limited alternative delivery resources to customers.		4
4. Endpoint storage facility—Major tank farm for large metropolitan area, airport and other party pipeline connection.	Serves large metropolitan area. Several million retail customers plus major international airport. Area served by other sources. Located in a sparsely populated industrial area.		2
5. River Span Block Valve	Block valve is upstream from above ground river span (see item 7). Breach could cause release of pipe volume into river and impact public safety and significant contamination to the water supply of a major metropolitan center. Restoration costs significant due to river spill clean up and difficult access to valve. Short timeframe to repair.		5
6. River Span Pipeline (Above Ground)	Above ground river span (see 1 above). Breach could release significant product into river and contaminate public water supply to a major metropolitan center. Block valve used as active mitigation, if not damaged. Significant public safety concern due to frequent recreational and commercial use on river. Long-term repair timeframe and significant repair costs and spill clean up costs. No alternate mode to market. Significant service interruption.		5
7. Inter-modal Terminal	Large inter-modal products terminal with rail, truck and pipeline service. Serves large metropolitan area. Provides gasoline to retail market, jet fuel to 2 major international airports and USAF. Large-scale damage would take months to repair. Repair costs would be significant. Significant disruption to local economy and possible national defense. No significant environmental impact. Limited public safety and employee impact.		4

## Form 2: Threats Worksheet

Facility Name: 1. Fictitious Pipeline Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Threat Ranking
Disgruntled Employee or Contractor	INT	No evidence of sabotage has been discovered in the past.	Minimal acts of sabotage or workplace violence.	Sabotage to equipment including SCADA causing possible release of hazardous materials, contamination of products, environmental impact, or major equipment damage and business interruption. Possible for nuisance threats, particularly from contract workers with intent to disrupt operations.	Insider access, knowledge and ability to operate independently with authorization and without question. May have access to keys, computer passwords, gate access codes, communication equipment, records, vehicles, proximity cards for access cards, company process control system.	Nuisance adversary is intent to cause inconvenience and financial impacts to the company or their employer. If very disgruntled or troubled, intent and motivation could be extreme to cause maximum damage, possibly with personal sacrifice as evidenced in various national workplace violence cases.	4

Form 3: Attractiveness/Target Ranking Form  
Facility Name: 1. Fictitious Pipeline Company

Critical Assets	Function/Hazards/ Criticality	S	Asset Attractiveness					A3	TR
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale		
3. DEF Branch and inter-modal terminal—Branch line providing mixed products to multi-modal marketing terminal, breakout facility, interconnection to other pipelines and direct connect to military, commercial airports and power plant.	Possible onsite fatalities. Possible offsite environmental impact. Limited alternative delivery resources to customers.	4	Major disruption to air travel, power supply and military. Easy access.	3	Some insider insight helpful but not necessary.	2	Public Image impact due to press/media interest.	3	TR 3
4. Endpoint storage facility—Major tank farm for large metropolitan area, airport and other party pipeline connection.	Serves large metropolitan area. Several million retail customers plus major international airport. Area served by other sources. Located in a sparsely populated industrial area.	2	Hardened facility. Access difficult but impact significant.	3	Insider information very helpful both to gain access and operational.	2	Nuisance issue with trespassing. Public image impact. Operational knowledge needed.	2	TR 3
5. River span block valve	Block valve is upstream from above ground river span (see item 7). Breach could cause release of pipe volume into river and impact public safety and significant contamination to the water supply of a major metropolitan center. Restoration costs significant due to river spill clean up and difficult access to valve. Short timeframe to repair.	5	Public safety and drinking water contamination. Perhaps included with attack on asset—River Span (above ground).	2	Some insider insight helpful but not necessary. Difficult access within minimal success.	1	Limited interest.	2	TR 2

## Form 4—Scenario Based Vulnerability

Facility Name: 1. Fictitious Pipeline Company

Critical Assets: 6. River Span Pipeline (Above Ground)

Scenario Worksheet Form											
Security Event Type	Threat Category	Type	Undesired Act	Consequences	S	Existing Safeguards/Countermeasures	Vulnerability	V	L	R	Recommendations
1.1. Destruction of span, release of product and loss of containment.	Terrorist	I/E/C	Destruction of river span by bombing.	Damage of river span; release of product into river; contamination of public drinking water supply; loss of service to downstream facilities for an extended period.	S5	1.1. Fencing around cable platform.	1. There are some protective measures; river span remote; easy access - above grade.	4	L3		1. Consider additional hardening to prevent access to river span.
						1.2. Air patrol and ground observation.					2. *Evaluate additional intrusion detectors feasible at this site.
						1.3. Manually operated block valve.					3. *Evaluate if CCTV is feasible.
						1.4. Monitoring pipeline conditions and flow ctrl.					4. Consider additional surveillance of this area.

\*Note: Additional countermeasures should be based on threat and criticality of the equipment / system under evaluation. Due to remote locations, electric power may not be available or feasible to implement electronic security measures.

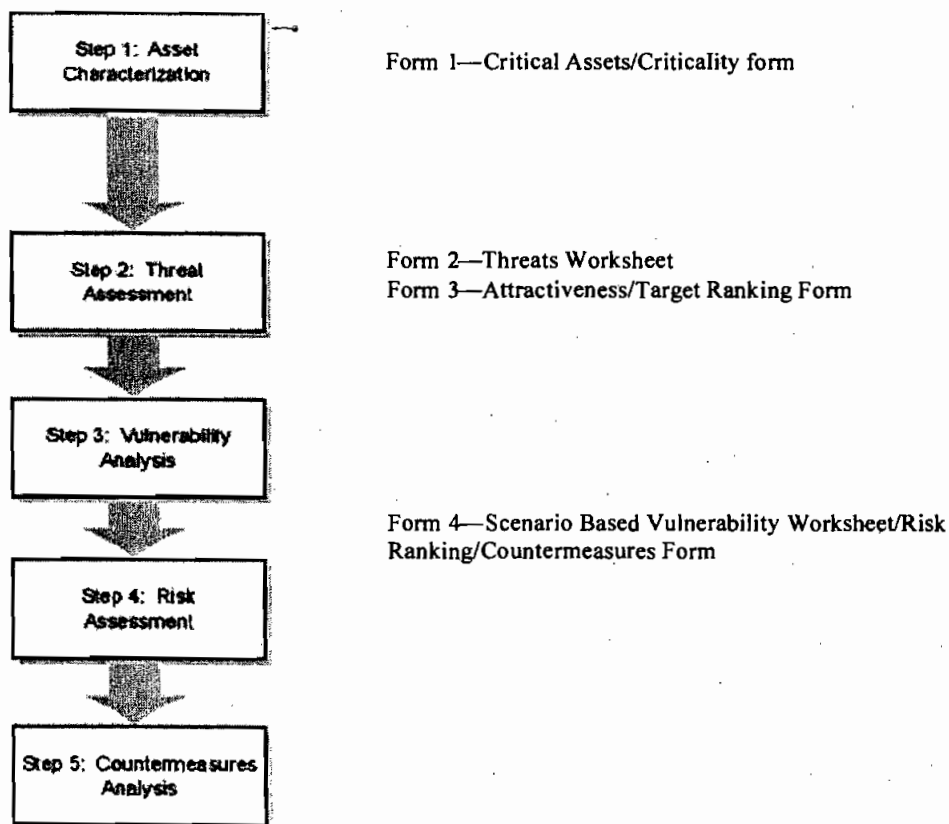
## Appendix C3—Fictitious Truck Transportation SVA Example

The application of the SVA Methodology to a fictitious products distribution system by truck is illustrated in the following example. Only the first page of each of the four forms is shown for illustrative purposes. It is assumed that the study is conducted by the owner of the trucking company and considers the various interfaces with customers and suppliers. However, the security of the customer and supplier facilities is the responsibility of the owners of those facilities.

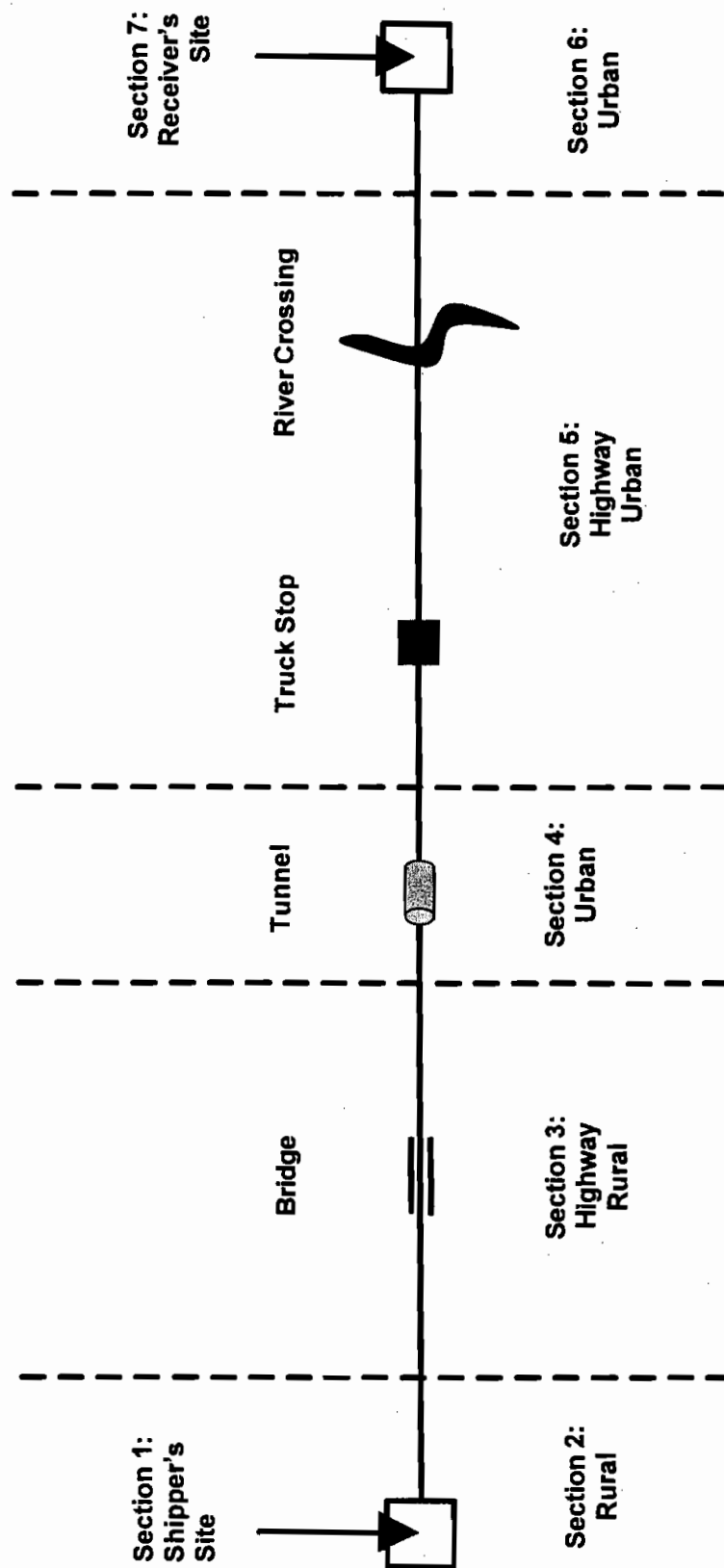
The example is of a fictitious hydrocarbon tank truck transportation system, which includes the tank truck, inventory of flammable liquids and the route specific variables such as the type of road, population centers and environmental receptors, and any stops. It is assumed that the shipper and receiver sites will have a separate SVAs. This example is intended to provide some insight on how one might conduct a security vulnerability analysis (SVA) using this methodology on the fictitious truck transportation system. This example is not intended to be all inclusive of every situation or every item that one may consider when conducting an SVA on a tank truck system. It is recognized that not all tank truck systems are the same. Factors such as route length, type of cargo, geographic location and many other factors play a significant role to determine the criticality of the transportation system thereby defining the type and level of analysis that may be appropriate for a particular situation.

The study is conducted in a top-down, systematic manner following the logic flowchart for the SVA as shown in Figure A. The five steps of the process are documented in four forms:

Figure A—SVA Methodology Flow Diagram



## SVA Methodology Fictitious Truck Transportation Example





## Form 2: Threats Worksheet

Facility Name: I. Fictitious Trucking Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Overall Assessment	Threat Ranking
International terrorists	I/E/C	I.I. No site-specific history of intentional acts against ACME.	According to information bulletins from DHS there have been suspicious activities involving bulk facilities including surveillance and following trucks. International terrorists have targeted trucks for highjackings and direct attacks.	Use of force to cause damage to vehicles while in transit or at loading/offloading facilities. This could cause a release of hydrocarbons and resulting fire and explosion with possible fatalities and injuries and degradation of transportation assets and environmental release. Terrorists may be interested in 1) weaponization of a tank truck to use fuels as a improvised, field-ready weapon at another location 2) directly damage the truck and cause collateral damage and disruption to the supply chain 3) "Trojan Horse" attack where the truck is used to introduce a weapon into a facility.	Assume a high level of organizational support; good resources; good financial backing; network of members; highly developed communication capabilities; weapons including small arms and explosives; possible vehicle bomb based on past events.	Assume adversary is highly motivated, likely extremist, prepared to die for their cause with intent to cause maximum damage to company assets including loss of life and economic disruption.	Credible threat. Include in analysis. An attempt to cause a violent attack on the truck would be consistent with both the tactics and goals of domestic terrorists.	3

## Form 2: Threats Worksheet

Facility Name: 1. Fictitious Trucking Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Overall Assessment	Threat Ranking
Disgruntled Employee or Contractor	INT	3.1. No evidence of sabotage has been discovered in the past. Have been several safety systems compromised and incidences of theft.	There have been acts of sabotage, theft and arson to the petroleum trucking operations in the past.	Sabotage to vehicles, including safety systems, arson, and theft of product.	Insider access, knowledge and ability to operate independently with authorization and without question. May have access to vehicles, facilities, gate access codes, communication equipment, records, and proximity cards for access cards.	Disgruntled employee is most-likely intent to cause inconvenience and financial impacts to the company or their employer. If very disgruntled or troubled, intent and motivation could be extreme to cause maximum damage, possibly with personal sacrifice as evidenced in various national workplace violence cases.	Credible threat. Include in analysis.	2

Form 3: Attractiveness/Target Ranking Form  
Facility Name: 1. Fictitious Trucking Company

Critical Assets	Function/Hazards/ Criticality	Asset Severity Ranking	Asset Attractiveness					TR
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contract or Attractiveness Rationale	A2	Activist Attractiveness Rationale	
4. Bridge along HWY 100.	Potential to block/damage bridge if tank truck attacked on the bridge.	3	Potential to cause major disruption to US Highway as well as result in potential fatalities and injuries.	3	No additional attraction.	1	Potential to block bridge.	TR3
5. Downtown section of route along State Route 5 (15 miles), traversing through high population density area.	Highest population density along route, but shortest segment.	3	High population density and potential to harm a large number of people.	3	No additional attraction.	1	No additional attraction.	TR3
6. Tunnel along State Route 5 leading into downtown.	Potential to block/damage tunnel preventing entrance/exit to the city and possible for multiple fatalities/injuries from occupants in other vehicles in tunnel.	3	High population impact potential as well as potential to disrupt local economy by blocking tunnel.	3	No additional attraction.	1	Potential to block tunnel.	TR3
7. HWY 200 (100 miles) traversing through primarily urban areas.	Longest stretch along the route with a high population density along the segment, potential to not only impact vehicle occupants on road but also surrounding population.	3	Long section of route provides access to truck highly populated area.	3	No additional attraction.	1	No additional attraction.	TR3
8. Truck Stop along HWY 200.	Potential for theft/access to unmanned vehicle.	3	Potential to gain access to truck-theft.	2	No additional attraction.	1	No additional attraction.	TR2
9. River Span along HWY 200.	Potential for environmental impact if product released into river.	2	Material not likely to cause sustained environmental impact.	1	No additional attraction.	1	No additional attraction.	TR1
10. Urban route off HWY 200 to Receiver's site - 10 miles.	Single entrance/exit to receiver's site, with potential for fatalities/injuries due to high population density surrounding the site.	2	Limited access due to shortness of route, but high population density makes section attractive.	2	No additional attraction.	1	No additional attraction.	TR2

## Appendix C4—Fictitious Rail Transportation SVA Example

The application of the SVA Methodology to a fictitious petroleum liquids pipeline system is illustrated in the following example. Only the first page of each of the four forms is shown for illustrative purposes. It is assumed that the study is conducted by the shipper company and considers the various interfaces with customers, suppliers and en-route interfaces. However, the security of the customer and supplier facilities and the en-route interfaces is the responsibility of the owners of those facilities, as well as the general route risk assessment issues. An example may include the switchyard security plan. It is the responsibility of the switchyard operator to ensure the security of the switchyard.

The general approach is to apply risk assessment resources and, ultimately, special security resources primarily where justified based on the SVA results. The SVA process involves consideration of the rail transportation system from both the general viewpoint and specific asset viewpoint. Consideration at the general overall route level is useful for determination of overall impacts of loss, infrastructure and interdependencies at the route level. The benefit of evaluating specific assets is that individual interface risks can be evaluated and specific countermeasures applied where justified in addition to more general countermeasures.

The SVA methodology uses this philosophy in several ways. The method is intended to be comprehensive and systematic in order to be thorough. First, it begins with the SVA team gaining an understanding of the entire rail transportation route that applies to the route that the shipper's products take through the value chain from production facility to various customers and end users. The SVA will analyze the critical assets that comprise the transportation system, the critical functions of the system, and the hazards and impacts if these assets or critical functions are compromised. This results in an understanding of which assets and functions are "critical" to the business operation. Criticality may be defined both in terms of the potential impact to the workers, community, the environment and the company, as well as to the business importance and continuity of the system. For example, a rail loading station or a specific branch along the route may be a critical part of the operation of the system due to inability to operate without it or, if attacked, it has the greatest impact. As such it may be given a high priority for further analysis and special security countermeasures.

Based on this first level of screening from all assets to critical assets, a critical asset list is produced. Next, the critical assets are reviewed in light of the threats. Adversaries may have different objectives, so the critical asset list is reviewed from each adversary's perspective and an asset attractiveness ranking is given. This factor is a quick measure of whether the adversary would value damaging, compromising, or stealing the asset, which serves as an indicator of the likelihood that an adversary would want to attack this asset and why.

If an asset is both critical (based on value and consequences) and attractive, then it is considered a "target" for purposes of the SVA. A target may optionally receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities. As shown in Figure A, all assets receive at least a general security review. This is accomplished by the basic SVA team's consideration as an asset to begin with, along with a baseline security survey. General security considerations may be found in security references such as the countermeasures checklist provided in Appendix F.

The study is conducted in a top-down, systematic manner following the logic flowchart for the SVA as shown in Figure A. The five steps of the process are documented in four forms:

**Form 3—Attractiveness/Target Ranking Form**

Columns 1 – 3 are repeated from Form 1 for reference. Column 4 is a documented rationale for why the particular asset or operation is attractive (or unattractive) and Column 5 is a ranking of that attractiveness on a relative Attractiveness Ranking scale or equivalent. This is repeated for other adversaries. Column 10 is an overall Target Ranking per the same scale, and is normally considered to be the highest attractiveness of any of the individual adversary rankings but also considers that the sum the different adversary's interests may make the asset more attractive. The Target Ranking is used to judge the degree of attractiveness of the target considering all the adversaries.

**Form 4—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form**

Column 1 is the Security Event Type (generally one of four security events including loss of containment, degradation of the asset, theft, or contamination); Column 2 is the Threat Category (adversary type such as terrorist, activist, employee); Column 3 is the Type of Adversary Attack (Insider/External); Column 4 is the Undesired Act (the assumed attack scenario, generally taken from the Threats Worksheet Columns 5, 6, 7); Column 5 is the Consequences; Column 6 (S) is the Severity Ranking from the Severity Ranking scale; Column 7 is the Existing Countermeasures, which considers the Deter, Detect, Delay, and Respond philosophy; Column 8 is the Vulnerability, which also considers the weaknesses or missing elements of the security strategy specific to the scenario; Column 9 is the Vulnerability Ranking per the Vulnerability Ranking scale; Column 10 is the Likelihood ranking (L) using the Likelihood scale, which is a judgment of the team considering the factors of Vulnerability, Threat, and Attractiveness; Column 11 is the Risk ranking (R) per the referenced Risk Ranking Matrix values; and Column 12 is the New /Countermeasures suggestions (where the risk is considered significant enough to justify the need for change).

**Responsibilities**

This example includes a sampling of assets that may be owned or operated by various parties. The responsibilities for conducting the SVA and for providing security need to be determined and may not solely be with the Shipper. It is recommended that the SVA include the appropriate parties to fully analyze the security issues, and that the results are discussed with railroad owner/operators, owner/operators of adjacent facilities and infrastructure providers as required for risk communication and completeness.

## Form 1: Critical Assets/Criticality Form

Facility Name: 1. Fictitious Rail Company

Critical Assets Form		
Critical Assets	Criticality/Hazards	Asset Severity Ranking
1. 25 railcars of petroleum products.	Two trains comprised solely of 25 petroleum products railcars are shipped daily from the shipper's terminal. After leaving the terminal the tankcars are divided into three separate trains at the switchyard and sent to three final receiver's sites. Site #1 - 25 railcars per day. Site #2 - 10 railcars per day. Site #3 - 15 railcars. En route from the switch yard to Site #1 is on a mainline track along a mostly rural area. En route to Site #2 and #3 crosses a river and have access to a siding as needed. The route to Site #2 branches off on an urban mainline, while the route to Site #3 continues through a tunnel before reaching its final destination. Potential hazard for this route is the potential to release one or more railcars resulting in a large environmental impact and or fire and subsequent fatalities and injuries if ignited.	4
2. Rural section of track to switch yard - 25 miles from shipper's site.	Single rail entrance/exit to supplier's site; incident involving railcar on this section of the route would result in limited fatalities/injuries due to low population density, but large fire could damage rail line.	3
3. Mainline section of track in rural area - 200 miles. Including rail spur to Receiver Site #1.	Long stretch across rural section of route.	3
4. Switch Yard	Switch point to individual trains to receiver's sites. Potential to damage site, other railcars and various products if petroleum products released and ignited.	4
5. River crossing	Potential for environmental impact if product released into river.	3
6. Mainline section of track in urban area - 300 miles. Including rail spurs to Site #2 and Site #3.	Long stretch across urban section on route to Site #2 and Site #3.	3
7. Siding in Urban Area (see 6)	Potential for theft/access to unmanned railcars.	4
8. Tunnel in Urban Area (see 6)	Potential to block/damage tunnel.	4

## Form 2: Threats Worksheet

Facility Name: 1. ACME Rail Company

Adversary Types	Source	Site Specific Threat	Threat History	Potential Actions	Adversary Capability	Adversary Motivation	Overall Assessment	Threat Ranking
Disgruntled Employee or Contractor	INT	3.1. No evidence of sabotage has been discovered in the past.	There have been acts of sabotage, theft and arson to the petroleum railcar operations in the past.	Sabotage to railcars including safety systems, and arson.	Insider access, knowledge and ability to operate independently with authorization and without question. May have access to railcars/train, facilities, gate access codes, communication equipment, records, and proximity cards for access cards.	Disgruntled employee is most-likely intent to cause inconvenience and financial impacts to the company or their employer. If very disgruntled or troubled, intent and motivation could be extreme to cause maximum damage, possibly with personal sacrifice as evidenced in various national workplace violence cases.	Credible threat. Include in analysis.	4

## Form 3: Attractiveness/Target Ranking Form

Facility Name: 1. Fictitious Rail Company

Critical Assets	Function/Hazards/ Criticality	S	Asset Attractiveness					A3	TR
			Foreign/Domestic Attractiveness Rationale	A1	Employee/Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale		
4. Switch Yard	Switch point to individual trains to receiver's sites. Potential to damage site, other railcars and various products if petroleum products released and ignited.	2	Potential to cause major disruption to rail transportation systems.	3	No additional attraction.	1	Potential to block bridge.	2	TR 3
5. River crossing	Potential for environmental impact if product released into river.	2	Potential contamination of drinking water supply and major disruption to rail transportation system.	3	No additional attraction.	1	No additional attraction.	1	TR 3
6. Mainline section of track in urban area – 300 miles. Including rail spurs to Site #2 and Site #3.	Long stretch across urban section on route to Site #2 and Site #3.	3	High population density and potential to harm a large number of people. Ability to disrupt Sites #2/3	4	Ability to disrupt Sites #2/3	4	Ability to disrupt Sites #2/3	2	TR 4
7. Siding in Urban Area (see 6)	Potential for theft/access to unmanned railcars.	3	Siding provides access to unmanned railcars in populated area.	3	No additional attraction.	1	No additional attraction.	1	TR 3
8. Tunnel in Urban Area (see 6)	Potential to block/damage tunnel.	3	Potential to cause major disruption to rail transportation system.	2	No additional attraction.	1	No additional attraction.	1	TR 2



## References

- "Chemical Accident Prevention Provisions" (part 68 of Title 40 of the *Code of Federal Regulations (CFR)*).
- Chemical Facility Vulnerability Assessment Methodology, NIJ Special Report, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, July, 2002.
- Counterterrorism and Contingency Planning Guide*. Special publication from Security Management magazine and American Society for Industrial Security, 2001.
- Guidance Document for Implementing 40 CFR Part 68, USEPA, 1998.
- Guidelines for Chemical Process Quantitative Risk Analysis*, Second Ed., Center for Chemical Process Safety, American Institute of Chemical Engineers, 2000.
- Guidelines for Consequence Analysis of Chemical Releases*, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1999.
- Guidelines for Technical Management of Chemical Process Safety*, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1998.
- Guidelines for Technical Planning for On-Site Emergencies*, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1996.
- Inherently Safer Chemical Processes – A Life Cycle Approach*, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1996.
- Layers of Protection Analysis*, Center for Chemical Process Safety, American Institute of Chemical Engineers, 2001.
- "Site Security Guidelines for the U.S. Chemical Industry", American Chemistry Council, October, 2001.
- Bowers, Dan M., "Security Fundamentals for the Safety Engineer", *Professional Safety*, American Society of Safety Engineers, December, 2001, pgs. 31-33.
- Dalton, Dennis. *Security Management: Business Strategies for Success*. (Newton, MA: Butterworth-Heinemann Publishing, 1995).
- Fischer, Robert J. and Green, Gion. *Introduction to Security*, 6th ed. (Boston: Butterworth-Heinemann, 1998).
- Ragan, Patrick T., et al., "Chemical Plant Safety", *Chemical Engineering Progress*, February, 2002 pgs. 62-68.
- Roper, C.A. *Physical Security and the Inspection Process* (Boston: Butterworth-Heinemann, 1997).
- Roper, C.A. *Risk Management for Security Professionals* (Boston: Butterworth-Heinemann, 1999).
- Walsh, Timothy J., and Richard J. Healy, eds. *Protection of Assets Manual* (Santa Monica, CA: Merritt Co.). Four-volume loose-leaf reference manual, updated monthly.

